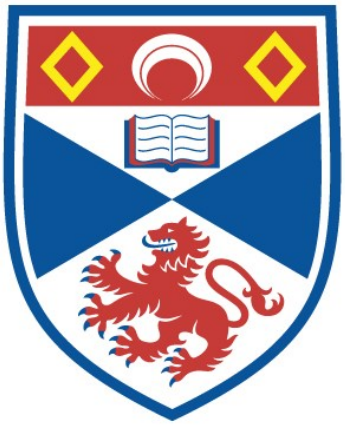
PRESENTATIONS OF LINEAR GROUPS

Peter D. Williams

A Thesis Submitted for the Degree of PhD
at the
University of St Andrews



1983

PRESENTATIONS OF LINEAR GROUPS

by

Peter D. Williams

A thesis submitted for the degree of doctor of philosophy of the University of St. Andrews.

Department of Pure Mathematics,
University of St. Andrews.

October 1982.

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 – 1346

ABSTRACT

Presentations of Linear Groups

by

Peter D. Williams.

If d(M) denotes the rank of the Schur multiplicator of a finite group G, then a group is efficient if -def G = d(M). Efficient presentations of the simple groups PSL(2,p), p an odd prime > 3, were obtained by J.G. Sunday ("Presentations of the groups SL(2,m) and PSL(2,m)." Can. J. Math. 24 (1972) 1129-1131). This raised the question of whether or not all finite simple groups are efficient.

In this thesis, we investigate the deficiency of the groups $PSL(2,p^n)$. J.A. Todd gave presentations for $PSL(2,p^n)$ which use large numbers of generators and relations ("A second note on the linear fractional group." J. London Math. Soc. 2 (1936) 103-107). Starting with these, we obtain, at best, deficiency -1 presentations for $PSL(2,2^n)$ ($\equiv SL(2,2^n)$) and deficiency -6 presentations for $PSL(2,p^n)$, p an odd prime. If $p^n \equiv -1 \pmod 4$, the latter can be reduced to a deficiency -4 presentation. Efficient presentations for PSL(2,25), PSL(2,27) and PSL(2,49) are obtained.

The Behr-Mennicke presentation for PSL(2,p) ("A presentation of the groups PSL(2,q)." Can. J. Math. 20 (1968) 1432-1438) is one of the most fundamental in the sense that it forms the basis for others, such as those given by Sunday, Zassenhaus (" A presentation of the groups PSL(2,p) with three defining relations." Can. J. Math 21, (1969) 310-311) and Sidki ("HK ∩ KH in Groups." Trabalho de Matematica, Number 96, Universidade de Brasilia (1975)). Behr and Mennicke derived their presentation indirectly, and it

would be desirable to have a more direct proof. The groups $G_p(a)$ are defined as

$$\langle U, R, S \mid U^3 = (UR)^2 = (US)^2 = S^p = R^t = (S^a RU)^3 = 1, S^{a^2} R = RS \rangle$$

where $a \in GF(p)^*$ and $a^{2t} \equiv 1 \pmod{p}$. We show that $G_p(2)$ is isomorphic with the Behr-Mennicke presentation for $PSL(2,p)$, $p > 3$. Conditions are found to discover when $G_p(a)$ is isomorphic with $PSL(2,p)$ and, under these conditions, this provides a direct proof of the Behr-Mennicke presentations.

For any odd positive integer m, we show that the groups $SL(2,\mathbb{Z}(m))$ and $PSL(2,\mathbb{Z}(m))$ are efficient. This corrects a technical mistake given in Sunday's paper.

Declaration

I declare that the following thesis is a record of research carried out by me, that the thesis is my own composition, and that it has not been accepted previously in application for a higher degree.

Peter D. Williams.

Declaration

I declare that I was admitted in October 1979 under Court Ordinance General Number 12 as a full time research student in the Department of Pure Mathematics.

Peter D. Williams.

Certificate

I certify that Peter David Williams has satisfied the conditions of the Resolution and Regulations and is thus qualified to submit the accompanying thesis in application for the degree of Doctor of Philosophy.

Edmund F. Robertson.

Preface

I wish to thank Dr. E.F. Robertson for his unflagging and enthusiastic supervision over the last three years, and for introducing me to the topic of group presentations. Also, my thanks to Dr. C.M. Campbell for many interesting discussions. I wish to thank the members of the Pure Mathematics Department for their kindness and encouragement. My thanks to Melinda Holtzman for her kind help in proof reading this thesis.

Finally, I am extremely grateful to the Science Research Council for their financial support over the last three years.

Contents

Introduction

Given a finite presentation $\langle X \mid R \rangle$ of a finite group G, the deficiency of the presentation is $|X| - |R| \leq 0$. The deficiency of G, def G, is the maximum deficiency over all finite presentations of G. A useful bound for def G is given in terms of the Schur Multiplicator of G, M(G). If d(G) is the minimum number of generators for G and d(M) the minimum number of generators of M(G), then the number of defining relations r, must satisfy $r \geq d(G) + d(M)$. Hence, $-\text{def } G \geq d(M)$. A group is efficient if $-\text{def } G = d(M)$.

Sunday [17] showed that the groups PSL(2,p) are efficient. His original presentation came from the two generator, four relation presentation for PSL(2,p) given by Behr and Mennicke in [2]. Campbell and Robertson [3] later produced a deficiency zero presentation for SL(2,p). The proof of the Behr-Mennicke presentation is rather indirect, and they state it would be desirable to have a more direct proof. In chapter two, we attempt to answer this question by generalizing Todd's presentation for PSL(2,p) [18], and obtain an interesting connection between the two presentations. We also look at the groups $PSL(2,\mathbb{Z}(m))$ and obtain efficient presentations for these.

The next step was to find if the groups $PSL(2,p^n)$, p a prime, $n \geq 2$, are efficient. In 1937, J.A. Todd [19] gave presentations for these groups. Unfortunately, they involved a large number of generators and relations (although they were of a simple form). Sinkov [16] managed to reduce Todd's presentations considerably, but still the number of defining relations increased with n. Two questions were raised. First, could we reduce the number of relations in these presentations? Secondly, Todd's presentations used a primitive element of $GF(p^n)$ satisfying an irreducible

polynomial of degree n. In the light of chapter two, are these conditions necessary, or, if so, what groups do you obtain when these conditions are relaxed?

In chapter three, we look at $SL(2,2^n)$. We show that the Todd-Sinkov presentation can be reduced to having at most five defining relations on three generators. In some cases, this reduces to a deficiency -1 presentation. Under suitable circumstances, we show that a direct product of $SL(2,2^n)$ can be obtained from this presentation.

The case is similar with $PSL(2,p^n)$, p an odd prime. In chapter four we reduce the Todd-Sinkov presentation to show, that on four generators, at most thirteen defining relations are needed. If $p^n \equiv -1 \pmod 4$, this reduces even further.

We produce a presentation for $PSL(2,p^2)$ in chapter five (based on the Todd-Sinkov presentation) but without using a primitive element of $GF(p^2)$. The generalization of this to other cases still evades us. Finally, we show that the groups PSL(2,25), PSL(2,27) and PSL(2,49) are efficient and give efficient presentations for them.

Chapter one is a collection of results and definitions to be used in later chapters.

Notation

$G \times H$	direct product of G and H.
$G \equiv H$	G isomorphic with H.
$\|G : H\|$	index of H in G.
C_n	cyclic group of order n.
C_∞	infinite cyclic group.
$H \leqslant G$	H a subgroup of G.
$Z(G)$	centre of G.
$\mathbb{Z}$	$\{..., -2, -1, 0, 1, 2, ...\}$
$\mathbb{N}$	$\{1, 2, 3, ...\}$
$\mathbb{Z}(m)$	integers modulo m.
$GF(p^n)$	field of order p^n.
$GF(p^n)^*$	non-zero elements of $GF(p^n)$.
(a,b)	highest common factor of a and b.
$a \mid b$ $(a \nmid b)$	a divides b (does not divide b)
$\oplus$	direct sum.
$\otimes$	tensor product.

Chapter I. Definitions and preliminary results

In this chapter we introduce some definitions and results to be used in later chapters. Two important subjects are the Schur Multiplicator and group 'algorithms'. Both play large parts in trying to obtain efficient presentations.

Let F be the free group on a set X, R a subset of F and N the normal closure of R in F.

Definition 1.1

If G is the factor group F/N we write $G = \langle X \mid R \rangle$ and call this a presentation of G. Elements of X are called generators and those of R, relators.

Definition 1.2

A group is finitely presented if X and R are both finite.

We shall only be concerned with finite presentations and assume all our presentations will be finite. The importance of presentations is stated in the following theorem.

Theorem 1.3 (see [10] page 24)

Every group has a presentation and every finite group is finitely presented.

It is far more convenient to work with relations rather than relators. If R, above, consists of the relators $r_1, r_2, \ldots, r_m$ then we obtain defining relations for G by setting each r_i equal to the identity and write

$$G = \langle X \mid r_i = 1,\ i = 1,2,\ldots,m \rangle .$$

We interpret this as G is the group generated by the elements of X subject to the relations $r_i = 1$, $i = 1,2,\ldots,m$ and think of this as a

presentation for G.

Definition 1.4

If $G = \langle X \mid R \rangle$ is a finite group, we define the deficiency of the presentation to be

$$|X| - |R| .$$

For finite groups, $|R| \geq |X|$. We therefore define the deficiency of G, def G, to be the maximum deficiency of all finite presentations of G.

We shall see shortly how def G is associated with the Schur Multiplicator of G. The next two theorems are of great importance. Their proof can be found in [10], p28-30.

Theorem 1.5 (von Dyck)

If R, S are subsets of the free group F on X with $R \subseteq S$ then there is an epimorphism

$$\theta : \langle X \mid R \rangle \longrightarrow \langle X \mid S \rangle$$

fixing X.

Theorem 1.6 (Substitution Test)

Suppose we are given a presentation $G = \langle X \mid R \rangle$, a group H and a mapping $\theta: X \longrightarrow H$. Then θ extends to a homomorphism $\theta': G \longrightarrow H$ if and only if, for all $x \in X$, for all $r \in R$, the result of substituting $x\theta$ for x in r yields the identity of H. Moreover, θ' is an epimorphism if the $x\theta$ generate H. In this case $|H| \leq |G|$.

Definition 1.7

Let k be a field (finite). The Special Linear group, SL(2,k), is the group of 2x2 matrices of determinant 1 with entries in k. The Projective Special Linear group, PSL(2,k) is defined as

$$PSL(2,k) = SL(2,k)/Z(SL(2,k))$$

Lemma 1.8

$Z(SL(2,k))$ is trivial if k has characteristic 2 and C_2 if k has characteristic p, p an odd prime.

Proof

If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(SL(2,k))$ then it commutes with all elements.

In particular, it commutes with $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

So, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -b & a \\ -d & c \end{pmatrix} \equiv \begin{pmatrix} c & d \\ -a & -b \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

which implies that $d = a$ and $c = -b$. Further,

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a+b \\ -b & a-b \end{pmatrix} \equiv \begin{pmatrix} a-b & a+b \\ -b & a \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

which gives $a-b = a$, i.e. $b = 0$. Also, as $ad - bc = 1$, we must have $a^2 = 1$. As k is a field, we require a to be 1 or -1. Thus the central elements are

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

When k has characteristic 2, these coincide.

Theorem 1.9

If $|k| = p^n$, then $|SL(2,k)| = p^n(p^n-1)(p^n+1)$ and

$$|PSL(2,k)| = \begin{cases} |SL(2,k)| & \text{if } p = 2 \\ |SL(2,k)|/2 & \text{for } p \neq 2 \end{cases}$$

Proof

This is a well known result and can be found in many texts, (for example see [8], p88). We shall count the matrices in $SL(2,k)$. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a matrix in $SL(2,k)$. We have $ad-bc = 1$.

$b = 0$, $c \neq 0$. Then $a = d^{-1}$. There are p^n-1 choices for a, since a is non-zero. c can be chosen in p^n-1 ways also. In total, $(p^n-1)^2$ matrices. Similarly when $b \neq 0$, $c = 0$ there are $(p^n-1)^2$ matrices.

For $b = c = 0$, then there are p^n-1 matrices. So we have

$$2(p^n-1)^2 + p^n-1$$

matrices with b or c = 0. Similarly, for a or d = 0.

Now for $a,b,c,d \neq 0$, we can choose a in p^n-1 ways. Since $a \neq d^{-1}$ (otherwise bc = 0), then d can be chosen in $p^n - 2$ ways. Also we can choose b in p^n-1 ways. c is determined from ad-bc = 1 since we know a,b and d. There are $(p^n-1)^2(p^n-2)$ matrices of this form, and we have exhausted all possibilities. Therefore,

$$\begin{aligned} |SL(2,k)| &= 2(2(p^n-1)^2 + p^n-1) + (p^n-1)^2(p^n-2) \\ &= (p^n-1)(4p^n-4 + 2 + p^{2n} - 3p^n + 2) \\ &= (p^n-1)(p^n + p^{2n}) \\ &= p^n(p^n-1)(p^n + 1). \end{aligned}$$

The order of PSL(2,k) follows from lemma 1.8 .

When $k = GF(p^n)$, we shall write $SL(2,p^n)$ and $PSL(2,p^n)$ rather than SL(2,k) and PSL(2,k).

The subgroup of upper triangular matrices is of special interest to us. As the order of $PSL(2,p^n)$ is $p^n(p^n-1)(p^n+1)/2$, for p odd, and $p \mid p^n$ but not p^n-1 or p^n+1, then $PSL(2,p^n)$ has a Sylow p-subgroup of order p^n. The set of matrices

$$S = \{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} ; y \in GF(p^n) \}$$

is such a subgroup. For each $t \in S$, $t = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$ we have $t^i = \begin{pmatrix} 1 & iy \\ 0 & 1 \end{pmatrix}$ and so $t^p = 1$. Let x be primitive in $GF(p^n)$. The elements

$$t_j = \begin{pmatrix} 1 & x^j \\ 0 & 1 \end{pmatrix} \quad j = 0,1,\ldots,n-1$$ are such that each generates a cyclic group of order p. S is the direct product of these n cyclic groups and so is abelian.

Let N(S) denote the normaliser of S. Any matrix in N(S) must

have the form $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ for,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 1-acy & a^2y \\ -c^2y & 1+acy \end{pmatrix} \in S$$

whenever $c = 0$. Also as $ad-bc = 1$, then $d = a^{-1}$. $|N(S)| = p^n(p^n-1)/2$. It follows that $|PSL(2,p^n): N(S)| = p^n+1$ and $|N(S): S| = (p^n-1)/2$ and that $N(S)$ is the subgroup of upper triangular matrices. Also, $S \trianglelefteq N(S)$ and $\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \in N(S)/S$. But this element has order $(p^n-1)/2$. $N(S)/S$ is therefore cyclic and so $N(S)$ is metabelian.

A similar result holds for $p = 2$ where $|PSL(2,2^n)| = 2^n(2^n+1)(2^n-1)$. Again, the upper triangular matrices form a subgroup of order $2^n(2^n-1)$.

Definition 1.10

The derived group G' of a group G is the subgroup generated by all elements of the form

$$[x,y] = x^{-1}y^{-1}xy, \qquad x,y \in G.$$

A group is perfect if $G = G'$.

Lemma 1.11 (see [12], p66-67)

G' is a normal subgroup of G with G/G' abelian. If $H \trianglelefteq G$ and G/H is abelian, then $G' \leqslant H$.

Lemma 1.12 (see [9], p181)

$SL(2,p^n)$ is perfect if $p^n>3$.

$SL(2,3)/SL'(2,3) \equiv C_3$.

We now discuss the Schur multiplicator of a group G.

Definition 1.13

Let G be a finite group with presentation $\langle X \mid R \rangle$. Let F be

the free group on X and N the normal closure of R in F. G = F/N. The Schur multiplicator of G, M(G), is defined as

$$M(G) = \frac{F' \cap N}{[F, N]} .$$

Definition 1.14

Let G be a finite group. If a group H has a subgroup A such that

(i) $A \leqslant H' \cap Z(H)$

(ii) $H/A \equiv G$

(iii) $|A| = |M(G)|$

then H is a covering group of G. If H satisfies (i) and (ii), then H is a stem extension of G.

Remarks

1. Note that (i) implies A is abelian since it is contained in the centre of H.

2. In a series of lectures at 'Groups St. Andrews, 1981', Professor J. Wiegold pointed out that this is not the only definition of the Schur multiplicator. The definition we have used is due to Hopf (Fundamentalgruppe und zweite Bettische Gruppe, Comm. Maths. Helvetici 14 (1941/42) 257-309). Another definition, due to W. Haebich, is that of a defining pair for G. A defining pair, (H,A), is such that (i) and (ii) above are satisfied. It can be shown that the orders of first members H, of defining pairs for G, are bounded. Those ~~The~~ A connected with H of maximum order are all isomorphic to M(G), and this can be used to define M(G). In terms of cohomology theory, M(G) is the factor group of the group of 2-cocycles by the the group of 2-coboundaries.

The next theorem is taken from [9] p631.

Theorem 1.15 (Schur) [14]

With the notation in definition 1.13, let $H = F/[N,F]$ and $T = N/[N,F]$, with $|X| = n$. Then,

(i) T is a finitely generated abelian subgroup of Z(H) and

$$M(G) = \frac{N \cap F'}{[N,F]}$$

is the torsion subgroup of T.

(ii) T has rank n.

(iii) If $T = L \times M(G)$ then H/L is a covering group of G.

(iv) If C is a covering group of G with $C/B \equiv G$, $B \leqslant Z(C) \cap C'$, then there is a homomorphism from $F/[N,F] \longrightarrow C$ and $B \equiv M(G)$.

Remarks

From above, M(G) is a finite abelian group and is independent of the presentation. From the definition of a covering group, not only is $|A| = |M(G)|$, but they are isomorphic.

The next result is adapted from a paper by Campbell and Robertson [4].

Theorem 1.16

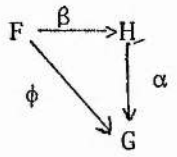
A stem extension H of a group G is a homomorphic image of some covering group of G.

Proof

Since H is a stem extension of G, there is a subgroup B, of H, with $B \leqslant Z(H) \cap H'$ and $H/B \equiv G$. B is contained in the Frattini subgroup of H, $\Phi(H)$. To see this, let $D = H' \cap Z(H)$ and assume $D \not\leqslant \Phi(H)$. Then there is a maximal subgroup A of H with $D \not\leqslant A$. $A \leqslant DA$ and so $DA = H$. If $h \in H$, then $h = da$, $d \in D$, $a \in A$. So,

$$h^{-1}Ah = a^{-1}d^{-1}Ada = a^{-1}Aa = A$$

since $d \in Z(H)$. Hence $A \trianglelefteq H$ and has index p (p a prime). Therefore, $H' \leqslant A$ (by lemma 1.11) and $D \leqslant H' \leqslant A$, gives the required contradiction. Let $G = F/R$. $F = \langle f_1, f_2, \ldots, f_n \rangle$, $G = \langle g_1, g_2, \ldots, g_n \rangle$ with $g_i = f_i\phi$, ϕ: $F \longrightarrow G$ the canonical epimorphism. If α is the canonical epimorphism from $H \longrightarrow G$, then there is an $h_i \in H$ with $h_i\alpha = g_i$. Then $H = \langle h_1, h_2, \ldots, h_n, B \rangle = \langle h_1, \ldots, h_n, \Phi(H) \rangle = \langle h_1, h_2, \ldots, h_n \rangle$, since $\Phi(H)$ can be removed from any generating set, (see[12], p186). This gives rise to an epimorphism β: $F \longrightarrow H$ with $f_i\beta = h_i$ such that the following diagram is commutative.



If $r \in R$, then $r\phi = 1$. But $r\phi = r\beta\alpha$ and so $r\beta \in \text{Ker } \alpha = B$. That is,

$$R\beta \subseteq B .$$

If $b \in B$, then $b\alpha = 1$. $\exists f \in F$ with $f\beta = b$ and so $f\phi = f\beta\alpha = 1$. Hence, $R\beta = B$. Also, $[R,F]\beta = [R\beta, F\beta] = [B,H] = 1$ since $B \leqslant Z(H)$. β induces an epimorphism β': $F/[F,R] \longrightarrow H$. Let $\overline{F} = F/[F,R]$ and $\overline{R} = R/[F,R]$, so that $M(G) = \overline{F'} \cap \overline{R}$.

Now, $M\beta' = (F' \cap R)\beta = F'\beta \cap R\beta = H' \cap B = B$. Since $R\beta = B$, we have $\overline{R}\beta' = B$. So if $r \in \overline{R}$, then there is an $m \in M$, with $m\beta' = r\beta'$, i.e. $(rm^{-1})\beta' = 1$. Let $N = \text{Ker } \beta'$.

$$r = (rm^{-1})m \in NM$$

and so $\overline{R} \subseteq NM$. But, Ker $\beta' \subseteq \overline{R}$, $M = \overline{F'} \cap \overline{R} \subseteq \overline{R}$, which implies that $NM \subseteq \overline{R}$ and so $NM = \overline{R}$.

As $$\frac{N}{N \cap M} = \frac{NM}{M} \equiv \frac{\overline{R}}{\overline{F'} \cap \overline{R}} \equiv \frac{R}{F' \cap R} \equiv \frac{RF'}{F'} < \frac{F}{F'}$$

then $N/(N \cap M)$ is free abelian. $N \cap M$ is a direct factor of N, that is $N = (N \cap M) \times E$. However, $\overline{R} = E \times M$ since $\overline{R} = NM = ((N \cap M) \times E)M$

which shows $\overline{R} = EM$. Also, $E \cap M \subseteq N \cap M$, $E \cap M \subseteq E$ so that

$$E \cap M \subseteq [N \cap M] \cap E = 1.$$

Now, $\overline{F}/E$ is a covering group of G for;

(i) $\dfrac{\overline{F}/E}{\overline{R}/E} \equiv \overline{F}/\overline{R} \equiv F/R \equiv G.$

(ii) $\overline{R}/E = \dfrac{ExM}{E} \equiv M.$

(iii) $M \leqslant \overline{F}'$ since $\dfrac{F' \cap R}{[F,R]} \leqslant F'/[F,R]$. Since $\overline{R} = EM$ then

$\overline{R}/E \leqslant (\overline{F}/E)'$. As $[\overline{R},\overline{F}] = 1$, we have $\overline{R}/E \leqslant Z(\overline{F}/E)$.

Finally, H is a homomorphic image of the covering group $\overline{F}/E$. For, $E \leqslant N = \text{Ker } \beta'$. $\beta' : \overline{F} \longrightarrow H$ induces an epimorphism, $\beta'' : \overline{F}/E \longrightarrow H$.

Corollary 1.17 [14]

G has a unique covering group when

$$(\,|G/G'|,\ |M(G)|\,) = 1.$$

Theorem 1.18 [9],p650

$$M(GxH) \equiv M(G) \times M(H) \times (G \otimes H).$$

If $(\,|G/G'|,\ |H/H'|\,) = 1$, then

$$M(G \times H) = M(G) \times M(H).$$

The multiplicators of SL(2,k) and PSL(2,k) are given in the following theorem.

Theorem 1.19 (see [9], p646)

$M(SL(2,p^n)) = 1$ except for $p^n = 2^2$ and 3^2.

$$|M(PSL(2,p^n))| = \begin{cases} 2 & p > 2,\ p^n \neq 3^2 \\ 1 & p = 2,\ p^n \neq 2^2 \\ 2 & p^n = 2^2 \\ 6 & p^n = 3^2 \end{cases}$$

For $p^n \neq 2^2, 3^2$, $SL(2,p^n)$ is a covering group of $PSL(2,p^n)$. For $p^n > 4$, $p^n \neq 3^2$, $SL(2,p^n)$ is the unique covering group of $PSL(2,p^n)$. $SL(2,5)$ is the covering group of $PSL(2,4)$.

A connection between the Schur multiplicator and def G is expressed in the next result.

Theorem 1.20(see [9], p642).

Let G be a finite group. Let d(M) denote the minimal number of generators of M(G). If $G = \langle X | R \rangle$ with $|R| = r$ then

$$r \geq |X| + d(M).$$

Definition 1.21

A finite group G is efficient if def G = -d(M).

In order to show a group is efficient it is enough to find a presentation of G on k generators and k + d(M) relations. We have from theorem 1.19 and definition 1.21, the following result.

Theorem 1.22

$PSL(2,p^n)$ is efficient if

$$-\operatorname{def}(PSL(2,p^n)) = \begin{cases} 1 & p \text{ an odd prime, } p^n = 2^2 \\ 0 & p = 2,\ p^n \neq 2^2. \end{cases}$$

We saw in lemma 1.12 that $SL(2,p^n)$ is perfect except for $p^n = 3$. It follows that $PSL(2,p^n)$ is perfect, $p^n \neq 3$. One of the checks, to see whether or not a presentation is one for $PSL(2,p^n)$, is to find whether or not the group presented is perfect. As we shall see,

this is most important when trying to obtain an efficient presentation. We describe two ways of finding $|G/G'|$, but they are in effect the same. First of all, we need the following result, (see [10], p 57).

Theorem 1.23

Given a finitely generated abelian group G, there are integers $s,n > 0$, and integers $d_i \geq 2$; $1 \leq i \leq s$, each dividing its successor such that

$$G \equiv C_{d_1} \times C_{d_2} \times \ldots \times C_{d_s} \times \underbrace{C_\infty \times C_\infty \times \ldots C_\infty}_{n \text{ copies}}$$

Further, s, n and the d_i, are all determined by G. n is called the torsion free rank of G and the d_i are called the invariant factors.

The first method for finding G/G', is as follows:

Theorem 1.24 [10],p51.

If $G = \langle X \mid R \rangle$, then a presentation for G/G' is $\langle X \mid R,C \rangle$, where if $X = \{x_1, x_2, \ldots, x_n\}$ then

$$C = \{ [x_i,x_j] = 1,\ 1 \leq i < j \leq n \}.$$

We know G/G' is abelian, and so once we have found a presentation for G/G', we can manipulate the relations to find $|G/G'|$.

Example 1.25

Find $|G/G'|$ where

$$G = \langle x, y, z \mid x^3 = y^3,\ zxz^{-1} = y,\ (zx)^3 = (zy)^2 = 1 \rangle$$

A presentation for G/G' is

$\langle x, y, z \mid x^3 = y^3,\ x = y,\ z^3x^3 = z^2y^2 = [x,z] = [y,z] = [x,y] = 1 \rangle$

Since $x = y$, then $z^2x^2 = 1$ implies $x^2 = z^{-2}$, and using $z^3 = x^{-3}$ we deduce that $z = x^{-1}$. Our relations reduce to $x = y = z^{-1}$. G/G' is infinite cyclic as it is generated by one element, which does not have finite order.

The second method is a matrix method and can be quicker (for a wider account on this subject, see [10], p57).

Let $G = \langle X \mid R \rangle$, $X = \{ x_1, x_2, \ldots, x_n \}$, $R = \{ r_1, r_2, \ldots, r_m \}$

Construct the relation matrix, M, as follows. From the i^{th} relation, $r_i = 1$, the (i,j) entry is obtained by adding the exponents of the generator x_j, occurring in this relation. In the above example, M looks like

$$\begin{array}{c} \begin{matrix} x & y & z \end{matrix} \\ \begin{pmatrix} 3 & -3 & 0 \\ 1 & -1 & 0 \\ 3 & 0 & 3 \\ 0 & 2 & 2 \end{pmatrix} \end{array}$$

Let $t = \min\{n,m\}$. We can apply the following operations on the rows and columns of M.

(i) Interchange any two rows (columns). (ii) Add any integer multiple of one row (column) to another. These are called elementary row and column operations. These operations allow us to reduce M to the form (D 0) or $\begin{pmatrix} D \\ 0 \end{pmatrix}$ where D is a diagonal matrix $(d_1, d_2, \ldots, d_t)$, (see [6], p282). It can be arranged so that each d_i divides its successor and so any 1's occur in the beginning and any 0's at the end. The invariant factors of G/G' are the d_i's which are not 0 or 1. For the above example we have:

$$\begin{pmatrix} 3 & -3 & 0 \\ 1 & -1 & 0 \\ 3 & 0 & 3 \\ 0 & 2 & 2 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 3 & 3 \\ 0 & 2 & 2 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & 1 \\ 0 & 2 & 2 \end{pmatrix} \longrightarrow$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \longrightarrow$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Hence $G/G' \cong C_\infty$. The rank is $\min\{ 3,4 \} - 2 = 1$.

In order to make a presentation for a group efficient, it will be neccessary to remove relations, or change the generating set. The rules which govern what we may do to a presentation are known as Tietze transformations. There are four transformations.

T1. We can add any relation to the presentation which is a consequence of the original relations.

T2. We can remove a relation if it is implied by the other relations.

T3. We can remove a generator if it is expressible in terms of the others.

T4. We can add a new generator provided we express it as a word in the original generators.

These transformations give new presentations of the group we started with. A more detailed account is given in [10], p34-38.

We now come to the subject of group 'algorithms'. The main ones we need are the Todd—Coxeter coset enumeration algorithm and the modified Todd—Coxeter algorithm. A description of these is given in chapter 4 of [10]. The Todd-Coxeter coset enumeration, (CE), is a method for evaluating the index of a subgroup H in a finitely presented group G when H is finitely generated by words in the generators of G. In general, G will be finite, but it can be applied to infinite groups which have subgroups of finite index. CE is not really an algorithm. For, given that $|G : H|$ is finite, there is no bound for the number of steps needed to find the index, even if the index is 1. We give a brief outline of the method by working through an example.

Example 1.26

Find the index of $H = \langle\ xyx^{-1},\ xzx^{-1}\ \rangle$ in

$G = \langle\ x, y, z \mid x^3 = y^2 = z^2 = 1,\ xyx = yz\ \rangle$

We write the relations in the form $r_i = 1$. The last relation is

$xyxzy = 1$, since z and y have order 2.

We now construct seven tables. The first two are headed by the subgroup generators and will have only one row. If the length of the subgroup generator is n, (taking all exponents to be 1 or -1), the length of the table is n + 1. The first two tables look like:-

x	y	x^{-1}

x	z	x^{-1}

We now define cosets of H, using integers to represent them, and fill in these tables as follows.

Define H = 1. That is, H is coset number 1. Since

$$Hxyx^{-1} = Hxzx^{-1} = H,$$

then by putting 1 in the first position of the tables above, we deduce that the last position must also be a 1. This gives

x	y	x^{-1}
1		1

x	z	x^{-1}
1		1

We can read this as $1.xyx^{-1} = 1$. That is the action of xyx^{-1} on coset 1, is to map it into coset 1. We now fill in the rest of the table. Define coset 2 to be 1.x, i.e. 2 = 1x. This puts a 2 as the second entry in the tables above. Also, $2x^{-1} = 1$, and so we know the third entry above is 2 also. The tables become

x	y	x^{-1}
1	2	2	1

x	z	x^{-1}
1	2	2	1

and are complete. This gives us new information, namely $2y = 2$ and $2z = 2$.

The third table is a record of the information we know and is called the coset table. If we have an m generator group, the coset table contains 2m columns, each headed by a generator x_i or its inverse, x_i^{-1}. The coset table has as many rows as cosets we have defined. At present, in our example, the coset table looks like

coset	x	y	z	x^{-1}	y^{-1}	z^{-1}
1	2					
2		2	2	1	2	2

.

The remaining four tables, headed by the relators are set up as the subgroup generator tables except that these tables contain as many rows as cosets that have been defined. These tables are called the relation tables. The i^{th} row starts with coset i. Each time we define a new coset, we also construct a new row in each of the relation tables. The algorithm ends when every position in these tables has been filled in. The relation tables at present are

x	x	x
1		1
2		2

y	y
1	1
2	2

z	z
1	1
2	2

x	y	x	z	y
1				1
2				2

We note that the last entry in each row is the same as the first. This is because each relation is the identity, and so for any coset Hw, and each relator r, we have

$$Hw.r = Hw.1 = Hw \ .$$

Thus the action of r on the coset is to map the coset into itself. We now go along each row of each relation table, filling in cosets we know from the coset table.

x	x	x
1	2	1
2		2

y	y
1	1
2	2

z	z
1	1
2	2

x	y	x	z	y
1	2	2		1
2		1	2	2

The tables are not complete. So, we define a third coset.

Let $3 = 2.x \ .$

We have immediately that

$$1.x^3 = 1 \Rightarrow 1xx^2 = 1$$

$$\Rightarrow 2xx = 1$$

$$\Rightarrow 3x = 1.$$

So, x maps coset 3 into coset 1. This is readily seen from putting this information into the first relation table.

x	x	x	
1	2	3	1

(... denotes new information).

Since the row completes, we must have 3x = 1. From the fourth relation table, we also obtain new information.

x	y	x	z	y	
1	2	2			1
2	3	1	2	2	2
3					3

The second row is now complete and shows that 3y = 1. We enter this information into the coset table.

coset	x	y	z	x^{-1}	y^{-1}	z^{-1}
1	2			3	3	
2	3	2	2	1	2	2
3	1	1		2		

We now go along the rows of each relation table filling in this information.

x	x	x	
1	2	3	1
2	3	1	2
3	1	2	3

y	y	
1	3	1
2	2	2
3	1	3

z	z	
1		1
2	2	2
3		3

x	y	x	z	y	
1	2	2	3	3	1
2	3	1	2	2	2
3	1				3

From the second table, the first row completes, showing that 1y = 3. From the last table, the first row completes, showing that 3z = 3. With this information, from the last row of the last relation, we obtain,

x	y	x	z	y	
3	1	3	1	1	3

so that 1z = 1. The tables now complete and are as follows.

x	x	x	
1	2	3	1
2	3	1	2
3	1	2	3

y	y	
1	3	1
2	2	2
3	1	3

z	z	
1	1	1
2	2	2
3	3	3

x	y	x	z	y	
1	2	2	3	3	1
2	3	1	2	2	2
3	1	3	1	1	3

The coset table is;

coset	x	y	z	x^{-1}	y^{-1}	z^{-1}
1	2	3	1	3	3	1
2	3	2	2	1	2	2
3	1	1	3	2	1	3

.

So, $|G : H| = 3$.

In coset enumeration there is a condition known as coincidence. This is when we obtain contradictory information. For example, suppose from one row of a table we obtain ix = j, i and j cosets, while from another, we obtain ix = k, $j \neq k$. Suppose $j < k$. In this case, the cosets j and k are equal. We replace all occurrences of k by j, and delete all the k^{th} rows of the tables. This may lead to further coincidence, in which case we repeat the above process. After dealing with this coincidence, we continue as before until all the tables complete.

The modified Todd-Coxeter algorithm (MOD), not only finds the index of a subgroup H in a group G, but also yields a presentation for H on the generators of H. One important application of this is the case H = G. We can then obtain a new presentation for G. Again, we shall outline the method by a specific example.

Given a subgroup H of G, with $|G : H|$ finite, we can define an equivalence relation on G by $x \sim y$ if and only if $xy^{-1} \in H$. The equivalence classes are the cosets of H in G with the usual properties of equivalence classes, i.e. $Hx = Hy$ or $Hx \cap Hy = \emptyset$, for all $x,y \in G$. For each coset we can choose a coset representative and the set of coset representatives is called a transversal, T say. Since every $g \in G$ belongs to some coset we have $g = ht$ for some $h \in H$, $t \in T$.

Using the Todd-Coxeter algorithm we can construct a transversal T. In the above example we take 1 (the identity of G) to represent H. Since 2 = 1x, we take as coset representative of coset 2 the element x. Similarly, we take x^2 to be the coset representative of coset 3 as $3 = 2x = 1x^2$.

In the modified Todd-Coxeter algorithm the idea is to keep track of coset representatives rather than cosets. We take 1 as the representative of the subgroup H. Instead of $ix = j$ we have equations of the form $ix = hj$ where i and j are coset representatives, h is a word in the generators of H and x (or x^{-1}) is a generator of G. h is determined by the following four rules.

M1. If $ix = j$ is a definition of coset representative j, then take $h = 1$.

M2. If $ix = j$ comes from the completion of a subgroup generator table headed by $h = wxv$ (where w and v are words in the generators of G) and $1w = h_1 i$ and $1v^{-1} = h_2 j$ then,

$$1\ wxv = h1$$

$$h_1\ ix = h\ 1v^{-1} = h\ h_2 j$$

$$ix = h_1^{-1} h\ h_2 j.$$

M3. If $ix = j$ comes from the completion of a row in the relation tables headed by wxv where we know $kw = h_1 i$ and $kv^{-1} = h_2 j$

then we have

$$k\ wxv = k$$

$$k\ wx = kv^{-1}$$

$$h_1 ix = h_2 j$$

$$ix = h_1^{-1} h_2 j.$$

M4. In the case of coincidence we have $ix = h_1 j$ and $ix = h_2 k$, with $k > j$ say. $k = h_2^{-1} h_1 j$ and we replace all occurrences of k with j as before.

We now work through an example.

Example 1.27

Find a presentation for $H = \langle x,\ wx^2w^{-1} \rangle$ in

$G = \langle x, w \mid x^5 = w^2 = (wx)^3 = 1 \rangle$.

As before we set up the subgroup generator and relation tables. Let $x = a$ and $wx^2w^{-1} = b$. The subgroup generator tables are

x

w	x	x	w^{-1}

.

By M1 we have $1x = a1$. The first subgroup generator table is now complete. We define $2 = 1w$ and $3 = 2x$. The second table is now complete,

w	x	x	w^{-1}
1 | 2	3	2	1

giving the new information $3x = t2$ where t is some word in the generators of H to be determined.

As $1wxxw^{-1} = b1$, then $2xxw^{-1} = b1$. So $3x = b1w = b2$. Hence $3x = b2$.

The coset table is

	w	x	x^{-1}
1	1.2	a1	$a^{-1}1$
2	1.1	1.3	$b^{-1}2$
3		b2	1.3

.

We put this information into the relation tables.

	x	x	x	x	x	
1	1	1	1	1	1	1
2	3	2	3	2	2	2
3				3	3	3

	w	w	
1	2	1	1
2	1	2	2
3		3	3

	w	x	w	x	w	x	
1							1
2							2
3							3

The second row of the first relation table is complete and gives new information, namely $2x = t2$ where t is to be determined. Since $x^5 = 1$ in G, we have $2x^5 = 2$. So,

$$2x\ x\ x\ x\ x = 2$$

$$\Rightarrow 3x\ x\ x\ x = 2$$

$$\Rightarrow b^2\ 2\ x = 2$$

and so $2x = b^{-2}2$. As $2x = 1.3$, this gives rise to a coincidence and we deduce $3 = b^{-2}2$. We now replace all occurrences of 3 by 2 and delete the third rows of all tables. From the first row of the third relation table we have

w	x	w	x	w	x	
1	2	2	1	1	2	1

giving the new information $2x = t1$.

Now,
$$1wxwxwx = 1$$

$$2xwxwx = 1$$

$$b^{-2}1xwx = 1$$

$$b^{-2}a1wx = 1$$

$$b^{-2}at1 = 1.$$

Hence $t = a^{-1}b^2$ and so $2x = a^{-1}b^2 1$. Therefore, $1x^{-1} = b^{-2}a2$. As $1x^{-1} = a^{-1}1$ this gives rise to another coincidence and we deduce

$$2 = a^{-1}b^2a^{-1}1\ .$$

The coset table now reads

	w	x	x^{-1}
1	$a^{-1}b^2a^{-1}1$	a1	$a^{-1}1$

and the relation tables complete trivially. This shows that H = G.

We now obtain a presentation for H on the generators a and b. The defining relations for H are obtained from each row of the relation tables and from the 1-rowed subgroup generator tables as follows.

The coset representatives are elements of G. As each relation is the identity of G, i.e. $r_i = 1$, we have $kr_i = h_{k,r_i}k$ where h_{k,r_i} is a word in the subgroup generators. Therefore, $h_{k,r_i} = 1$ and is a relation involving the generators of H. Similarly, from the subgroup generator tables we have

$$1\,h_i = h_{1,h_i}\,1.$$

But as $1\,h_i = h_i\,1$ we have a further relation $h_i = h_{1,h_i}$.

From the first relation table we have

$$1x^5 = a\,1x^4 = a^2 1x^3 = a^5 1.$$

Therefore, in H, $a^5 = 1$. From the second relation table we have

$$1ww = a^{-1}b^2a^{-1}a^{-1}b^2a^{-1}1$$

giving $(a^{-2}b^2)^2 = 1$. From the third relation table,

$$1wxwxwx = a^{-1}b^2a^{-1}aa^{-1}b^2a^{-1}aa^{-1}b^2a^{-1}a1$$

and so $(a^{-1}b^2)^3 = 1$. We also obtain the relations from the subgroup generator tables as described above.

$1x = a1$ and $1x = a1$ gives the relation $a = a$.

$1wx^2w^{-1} = a^{-1}b^2a^{-1}aaab^{-2}a1$ and $1wx^2w^{-1} = b1$ gives the relation

$$a^{-1}b^2a^2b^{-2}ab^{-1} = 1.$$

Therefore,

$$G = \langle a, b \mid a^5 = (a^{-1}b^2)^3 = (a^{-2}b^2)^2 = a^{-1}b^2a^2b^{-2}ab^{-1} = 1 \rangle .$$

This can be simplified using Tietze transformations as follows.

$a^{-1}b^2a^{-1} = b^{-2}ab^{-2} \Rightarrow ab^{-2}a = b^{-2}ab^{-2} \Rightarrow b^2ab^{-2} = ab^{-2}a^{-1} \Rightarrow$

$b^2a^2b^{-2} = ab^{-4}a^{-1} \Rightarrow b^4 = ab^{-4}a.$

Therefore, $a^{-1}b^2a^2b^{-2}ab^{-1} = a^{-1}b^2b^2a^{-1}b^{-1} = b^{-4}b^{-1}$.

Hence,

$G = \langle a, b \mid a^5 = b^5 = (a^{-1}b^2)^3 = (a^{-2}b^2)^2 = 1 \rangle$.

Remarks

1. There was no column headed by w^{-1} in the coset table. Usually when there is an element of order two only one column is recorded. This is because $iw = hj \Rightarrow iww = hjw \Rightarrow h^{-1}i = jw$.
2. We chose to write one of the subgroup generators as wxw^{-1} even though w has order two. This was done to enable us to fill the subgroup generator tables before looking at the relation tables.

Computer implementations of the Todd-Coxeter coset enumeration algorithm are available. At the University of St. Andrews we have the Canberra suite of programs mounted on a Digital VAX-11/780 computer. The package contains a coset enumeration program. It also contains a computer implementation of the Reidemeister-Schreier algorithm (RS). This is another algorithm for finding a presentation of a subgroup of finite index in a group (see chapter 4 of [10]). This has the disadvantage that the resulting presentation is not on the original subgroup generators. The package also contains a program (TTRANS) which carries out Tietze transformations. This is invaluable as RS produces a large number of generators and relations.

Out of discussions over certain problems, TTRANS has been improved by the addition of certain subroutines. These new subroutines were written by Dr. E.F. Robertson. Where we have used these programs we shall refer to the program names which are:
COSET - Computer implementation of the Todd-Coxeter coset enumeration

algorithm.

RS - Computer implementation of the Reidemeister-Schreier algorithm.

TTRANS- Tietze transformation program.

ABEL - A program to aid calculation of $|G/G'|$.

We shall need the following results about elements which commute in a group.

Lemma 1.28

If, in a group, the elements x and y satisfy

$$x^m = y^n = [x^r, y^s] = 1$$

where $(r,m) = (s,n) = 1$, then $[x, y] = 1$.

Proof

Since x^r commutes with y^s, it commutes with all powers of y^s. Since $(s,n) = 1$, $a, b \in \mathbb{Z}$ with $as + bn = 1$. So x^r commutes with $y^{as} = y^{1-bn} = yy^{-bn} = y$. That is x^r commutes with y. Also, y

commutes with powers of x^r. As $(r,m) = 1$, then $\exists\, a', b' \in \mathbb{Z}$ with $a'r + b'm = 1$.

Hence y commutes with $x^{a'r} = x^{1-b'm} = x$.

Lemma 1.29

Let $u_1, u_2, \ldots, u_n$ be elements of a group which commute with one another. Let a, b, c, d be elements of the group which commute with each of the u_i's, and $[a,b] = 1$. Further, suppose

$$a = u_1 u_2 \ldots u_k c$$

and $$b = u_{k+1} u_{k+2} \ldots u_n d \ .$$

Then $[c,d] = 1$.

Proof

a and b commute so that

$$u_1 u_2 \ldots u_k c u_{k+1} u_{k+2} \ldots u_n d = u_{k+1} u_{k+2} \ldots u_n d u_1 u_2 \ldots u_k c \ .$$

As c and d commute with the u_i, this expression becomes

$$u_1 u_2 \ldots u_n cd = u_{k+1} u_{k+2} \ldots u_n u_1 u_2 \ldots u_k dc = u_1 u_2 \ldots u_n dc$$

since the u_i commute.

Therefore $$cd = dc.$$

The next result is a generalization of a result proved by Sidki [15].

Lemma 1.30

For any group G, suppose $\exists\, a, b \in G$ satisfying the relations

$$a^p = b^p = (a^n b^m)^2 = 1$$

where p is an odd prime, and $n, m \not\equiv 0 \pmod p$. Then a and b satisfy

$$(a^{2n} b^{m/2})^2 = 1 \Leftrightarrow (a^n b^{m/2})^3 = 1$$

where m/2 denotes $m(p+1)/2 \pmod p$.

Proof

Suppose $(a^n b^{m/2})^3 = 1$.

Then,

$$a^n b^{m/2} a^n = b^{-m/2} a^{-n} b^{-m/2}$$

$$= b^{-m/2} b^m a^n b^m b^{-m/2}$$

$$= b^{m/2} a^n b^{m/2}.$$

Therefore,

$$a^{2n} b^{m/2} \; a^{2n} = a^n \; b^{m/2} \; a^n \; b^{m/2} \; a^n = b^{-m/2}.$$

That is,

$$(a^{2n} b^{m/2})^2 = 1.$$

Conversely, suppose that

$$(a^{2n} \; b^{m/2})^2 = 1.$$

Then, $\forall\ k \in \mathbb{N}$,

$$a^n \; b^{m/2} a^n = a^{-(2k+1)n} \; b^{-m/2} \; a^{-n} \; b^{km} \qquad (1.1)$$

To show this, we see that

$$a^n \; b^{m/2} \; a^n = a^{-n} \; b^{-m/2} \; a^{-n}$$

$$= a^{-3n} \; a^{2n} \; b^{-m/2} \; a^{-n}$$

$$= a^{-3n} \; b^{-m/2} \; a^{-2n} \; b^{-m} \; a^{-n}$$

$$= a^{-3n} \; b^{-m/2} \; a^{-n} \; b^m,$$

showing (1.1) holds when $k = 1$.

Also,

$$a^{-(2k-1)n} \; b^{-m/2} a^{-n} \; b^{(k-1)m} = a^{-(2k-1)n} \; b^{-m/2} \; a^{-n} \; b^{-m} \; b^{km}$$

$$= a^{-(2k-1)n} \; b^{-m/2} \; b^m \; a^n \; b^{km}$$

$$= a^{-(2k-1)n} \; b^{m/2} \; a^n \; b^{km}$$

$$= a^{-(2k-1)n} \; b^{m/2} \; a^{2n} \; a^{-n} \; b^{km}$$

$$= a^{-(2k+1)n} \; b^{-m/2} \; a^{-n} \; b^{km}$$

provides the inductive proof. In particular, when $k = (p-1)/2$

then

$$a^{-(2k+1)n} = 1 \quad \text{and} \quad b^{km} = b^{-m/2}.$$

Therefore, (1.1) gives

$$(a^n b^{m/2})^3 = 1.$$

Lemma 1.31 (see [6a], p211 where this result is attributed to König and Rados)

Consider the equation

$$a_o + a_1 x + a_2 x^2 + \ldots + a_{q-2} x^{q-2} = 0$$

over GF(q), where $q = p^n$ for some prime p. Let C be the circulant matrix whose first row consists of the coefficients a_i. Then, the number of non-zero roots of the equation in GF(q) is q-1-r where r is the rank of C.

Proof

Consider the Vandermonde matrix

$$\begin{pmatrix} 1 & \beta_o & \beta_o^2 & \beta_o^3 & \ldots & \beta_o^{q-2} \\ 1 & \beta_1 & \beta_1^2 & \beta_1^3 & \ldots & \beta_1^{q-2} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta_{q-2} & \beta_{q-2}^2 & \beta_{q-2}^3 & \ldots & \beta_{q-2}^{q-2} \end{pmatrix}$$

where $\beta_i \in GF(q)^*$. Without loss of generality, we may take $\beta_o = 1$, β_1 to be a primitive element of GF(q) (β say) and $\beta_i = \beta^i$, $1 \leq i \leq q-2$. $\det V = \prod_{j<i} (\beta_i - \beta_j)$ (see [6], p 167). Since $\beta_i \neq \beta_j$ then $\det V \neq 0$. Therefore V has full rank. Let f(x) denote the right hand side of the equation in the statement of the lemma. Consider the product VC. The i^{th} row of V is,

$$(1, \beta^i, \beta^{2i}, \ldots, \beta^{(q-2)i})$$

while the j^{th} column of C is the transpose of

$$(a_{j-1}, a_{j-2}, \ldots, a_o, a_{q-2}, \ldots, a_j).$$

Thus, the (i,j) entry of VC is:

$$a_{j-1} + a_{j-2}\,\beta^{i} + a_{j-3}\,\beta^{2i} + \ldots + a_{o}\,\beta^{(j-1)i} + a_{q-2}\,\beta^{ji} + \ldots$$

$$\ldots + a_{j}\,\beta^{(q-2)i}.$$

$$= a_{o}\,\beta^{(j-1)i} + a_{1}\,\beta^{(j-2)i} + \ldots + a_{j-1} + a_{j}\,\beta^{(q-2)i} + a_{j+1}\,\beta^{(q-3)i}$$

$$+ \ldots + a_{q-2}\,\beta^{ji}$$

$$= \beta^{(j-1)i}\left(a_{o} + a_{1}\,\beta^{-i} + a_{2}\,\beta^{-2i} + \ldots + a_{j-1}\,\beta^{(1-j)i} + a_{j}\,\beta^{(q-2+1-j)i}\right.$$

$$\left. + a_{j+1}\,\beta^{(q-3+1-j)i} + \ldots + a_{q-2}\,\beta^{i}\right)$$

$$= \beta^{(j-1)i} \sum_{k=0}^{q-2} a_{k}\,\beta^{-ki} = \beta^{(j-1)i}\, f(\beta^{-i}).$$

Now, if β^{-i} is a root of $f(x)$, then the i^{th} row consists of all zeros. Hence, q-1-rank(VC) $\geq$ N, where N is the number of non-zero roots of the equation. It remains for us to show that the remaining q-1-N rows are linearly independent. Let $i_1, i_2, \ldots, i_k$ index these rows, k = q-1-N. Now row i_s is

$$f(\beta^{-i_s})(\,1,\ \beta^{i_s},\ \beta^{2i_s},\ \ldots,\ \beta^{(q-2)i_s})$$

which is a non-zero multiple of the i_s^{th} row of V. Hence, the rows $i_1, i_2, \ldots, i_k$ are linearly independent since det V $\neq$ 0.

Since V has full rank, then rank(VC) = rank(C) = r. Hence, N = q-1-r.

One trick we shall use frequently is the following.

Lemma 1.32

Let a and b be elements of a group, satisfying the relation

$$a\,b\,a^{-1} = b^{r},$$

for some $r \in \mathbb{Z}$. Then, $\forall\ s \in \mathbb{N}$,

$$a^{s} b\, a^{-s} = b^{r^{s}}.$$

Proof

The result clearly holds for $s = 1$. Assume for some $t \in \mathbb{N}$ that

$$a^t b\, a^{-t} = b^{r^t}.$$

Then,

$$a^{t+1} b\, a^{-1-t} = a\, b^{r^t} a^{-1}.$$

As $a\, b\, a^{-1} = b^r$, then $(aba^{-1})^n = ab^n a^{-1} = b^{rn}$. In particular, when $n = r^t$, $ab^{r^t} a^{-1} = b^{r.r^t} = b^{r^{t+1}}$. Hence the result holds for $t+1$. As the result holds for $t = 1$, then it holds for all $t \in \mathbb{N}$.

Chapter II. Presentations for PSL(2,p), p an odd prime.

J. A. Todd's presentation for PSL(2,p) [18] uses the existence of a primitive element of the field GF(p). A primitive element is such that it generates GF(p)* under multiplication. We generalize this presentation by removing the need for the element to be primitive, and obtain conditions for the resulting group to be PSL(2,p).

Using this new presentation, we attempt to answer a question posed by Behr and Mennicke [2], namely to find a more direct proof for their presentation of PSL(2,p). We investigate several presentations for PSL(2,p) and the connections between them, ending with a two generator, three relation presentation for PSL(2,p).

Finally, we look at PSL(2,$\mathbb{Z}(m)$) - the group of 2x2 matrices of determinant 1 with entries in the ring $\mathbb{Z}(m)$. We show that PSL(2,$\mathbb{Z}(m)$) is efficient. An efficient presentation is found by first of all obtaining a deficiency zero presentation for SL(2,$\mathbb{Z}(m)$).

In 1932, Todd [18] produced the following presentation for PSL(2,p), $p > 3$.

$$\langle U, R, S \mid U^3 = (UR)^2 = (US)^2 = R^t = S^p = 1, S^{a^2} R = RS \rangle \qquad (2.1)$$

where $t = (p-1)/2$, and a is a primitive element of GF(p). If $p \equiv 1 \pmod 4$, the extra relation

$$(S^a RU)^3 = 1 \qquad (2.2)$$

is required. This was a great improvement on earlier presentations such as that given by Moore (see [8], p300), as it required only six (or seven) defining relations. One problem that we shall investigate is whether or not the element a, in the above presentation, need be primitive.

Definition 2.1

We define the groups

$$G_p(a) = \langle\ U, R, S \mid U^3 = (UR)^2 = (US)^2 = R^t = S^p = (S^aRU)^3 = 1,$$
$$S^{a^2}R = RS\ \rangle \qquad (2.3)$$

where $a \in GF(p)^*$ and t is the order of a^2 in $GF(p)$.

We attempt to classify $G_p(a)$. We have immediately:

Lemma 2.2

If $a = \pm 1$, $G_p(a)$ is trivial. If a is a primitive element of $GF(p)$, then $G_p(a) \cong PSL(2,p)$.

Proof

If $a = 1$, then $SR = RS$. From $(SRU)^3 = 1$ we obtain

$$RSURSURSU = 1$$
$$RU^{-1}RURSU = 1 \qquad \text{(since } (US)^2 = 1\text{)}$$
$$RU^{-1}U^{-1}SU = 1 \qquad \text{(since } (UR)^2 = 1\text{)}$$
$$RUSU = 1$$
$$R = S.$$

But since $t \mid p-1$, then $(t,p) = 1$. $\exists\, \lambda,\mu \in \mathbb{Z}$ with

$$\lambda t + \mu p = 1.$$

Hence, $R^{\lambda t} = R^{1-\mu p} = R = 1$, since $S^p = 1$ and $R = S$.
Also, $(UR)^2 = U^2 = 1$, and as $U^3 = 1$, we deduce $U = 1$. Similarly, using $(US)^2 = S^2 = 1 = S^p$, we deduce $S = 1$. Hence $G_p(1)$ is trivial.

If $a = -1$, we still have $SR = RS$. Again, using $(S^{-1}RU)^3 = 1$, we obtain,

$$S^{-1}RURS^{-1}US^{-1}RU = 1$$
$$S^{-1}U^{-1}S^{-1}US^{-1}RU = 1 \qquad \text{(Using } (UR)^2 = 1\text{)}$$

$$U^{-1}S^{-1}RU = 1 \qquad \text{(using } (US)^2 = U^3 = 1\text{)}$$

and so R = S. As above, this implies U, R and S are trivial. If a is primitive in GF(p), then (2.3) is precisely Todd's presentation for PSL(2,p) when $p \equiv 1 \pmod 4$. For $p \equiv -1 \pmod 4$ it is easy to show using matrices that (2.2) holds in (2.1) and again $G_p(a) \equiv PSL(2,p)$.

It is convenient to change this presentation of $G_p(a)$ using Tietze transformations.

Lemma 2.3

The group $G_p(a)$, $a \neq \pm 1$, can be presentated as

$$\langle\ x, w, z \mid x^p = w^2 = z^t = (wx)^3 = (wz)^2 = (x^a zw)^3 = 1,\ x^{a^2}z = z\,x\ \rangle \qquad (2.4)$$

Proof

The defining relations for $G_p(a)$ in terms of generators U, R and S are

$$U^3 = (UR)^2 = (US)^2 = S^p = R^t = (S^aRU)^3 = 1,\ S^{a^2}R = RS.$$

Quite clearly $G_p(a) = \langle\ S, US, S^{-1}R\ \rangle$. If we let x = S, w = US and $z = S^{-1}R$, then using Tietze transformations the defining relations become:

$$x^p = w^2 = (xz)^t = (wx)^3 = (wz)^2 = (x^a zw)^3 = 1,\ x^{a^2}z = zx.$$

Now assume as an inductive hypothesis that

$$(xz)^k = x^{u(k)}\ z^k$$

where $u(k) = 1 + a^2 + a^4 + \ldots + a^{2(k-1)}$. It holds for k = 1. Then,

$$(xz)^{k+1} = x^{u(k)}\ z^k xz$$

But as $zxz^{-1} = x^{a^2}$, then $z^k x z^{-k} = x^{a^{2k}}$, using lemma 1.32.

Therefore, $(xz)^{k+1} = x^{u(k)} x^{a^{2k}} z^{k+1} = x^{u(k+1)} z^{k+1}$.

This provides the inductive step. In particular, when $k = t$, then

$$u(t) = 1 + a^2 + \ldots + a^{2(t-1)} = \frac{1 - a^{2t}}{1 - a^2} \equiv 0 \pmod{p}.$$

So $(xz)^t = z^t = 1$. This means we can replace $(xz)^t = 1$ by $z^t = 1$, and obtain the stated presentation.

Remark

When $a = \pm 1$, we have shown that $G_p(a)$ is trivial. However, if we put $a = \pm 1$ in (2.4), we obtain a presentation for the group

$$(2, 3, p) = \langle\ a, b \mid a^2 = b^p = (ab)^3 = 1\ \rangle$$

which is infinite for $p > 6$ (see [7]).

Lemma 2.4

In $G_p(a)$, $a \neq \pm 1$, the relations

$$(x^{a^n} z^n w)^3 = 1 \qquad n = 1, 2, \ldots$$

hold.

Proof

We use induction on n. The relation clearly holds for $n = 1$. Now,

$$x^{a^2} z^2 w\, x^{a^2} z^2 w\, x^{a^2} z^2 w = x^{a^2} z\, w\, z^{-1} x^{a^2} z\, w\, z^{-1} x^{a^2} z\, z\, w$$

$$= x^{a^2} z\, w\, x\, w\, x\, z\, w$$

$$= z\, x\, w\, x\, w\, x\, z\, w$$

$$= (zw)^2 = 1.$$

The relation holds for $n = 2$. Assume that for all $r \leq k$

$$(x^{a^r} z^r w)^3 = 1.$$

$$x^{a^{k+1}} z^{k+1} w\, x^{a^{k+1}} z^{k+1} w\, x^{a^{k+1}} z^{k+1} w =$$

$$= x^{a^{k+1}} z^{k+1} w\, z\, x^{a^{k-1}} z^{k} w\, x^{a^{k+1}} z^{k+1} w$$

$$= x^{a^{k+1}} z^{k} w\, x^{a^{k-1}} z^{k-1} w\, z^{-1}\, x^{a^{k+1}} z^{k+1} w$$

$$= x^{a^{k+1}} z\, z^{k-1} w\, x^{a^{k-1}} z^{k-1} w\, x^{a^{k-1}} z^{k-1} w\, z^{-1}$$

$$= x^{a^{k+1}} z\, x^{-a^{k-1}} z^{-1}$$

$$= 1.$$

As the relation holds for k+1, then it holds for all integers. Hence the result.

Theorem 2.5

Let $a \in GF(p)\setminus\{0, 1, -1\}$. For any $r \in \mathbb{N}$ such that $a^r \neq \pm 1$, there is an epimorphism

$$\phi' : G_p(a^r) \longrightarrow G_p(a).$$

Proof

We use the substitution test, theorem 1.6. By lemma 2.3, $G_p(a)$ and $G_p(a^r)$ are the groups

$$\langle x, z, w \mid x^p = w^2 = z^t = (wx)^3 = (x^a zw)^3 = (wz)^2 = 1,\ x^{a^2} z = zx \rangle$$

and

$$\langle b, c, d \mid d^p = c^2 = b^s = (cd)^3 = (d^{a^r} bc)^3 = (cb)^2 = 1,\ d^{a^{2r}} b = bd \rangle$$

respectively, where s is such that $a^{2rs} \equiv 1 \pmod p$. Consider the map ϕ: $\{b, c, d\} \longrightarrow G_p(a)$ given by

$b\phi = z^r$, $c\phi = w$, $d\phi = x$. Now $(d\phi)^p = x^p = 1$, $(c\phi)^2 = w^2 = 1$, $(c\phi d\phi)^3 = (wx)^3 = 1$, $(c\phi b\phi)^2 = (wz^r)^2 = 1$ (since $wzw = z^{-1}$). Also, $((d\phi)^{a^r} b\phi\ c\phi)^3 = (x^{a^r} z^r w)^3 = 1$, by lemma 2.4. $(b\phi)^s = z^{rs} = 1$, since $a^{2rs} = 1$ and so $t \mid rs$.

Therefore, by the substitution test, ϕ extends to a homo-

morphism ϕ': $G_p(a^r) \longrightarrow G_p(a)$. That ϕ' is an epimorphism follows from the fact that $\langle x, w \rangle = G_p(a)$. This may not seem obvious but will be shown in theorem 2.8.

Corollary 2.6

For $a \neq \pm 1$, $G_p(a)$ is non-trivial and has PSL(2,p) as a homomorphic image.

Proof

If a is primitive in GF(p), then $G_p(a)$ is PSL(2,p), and so every group $G_p(a^r)$, $a^r \neq \pm 1$, has PSL(2,p) as a homomorphic image.

Theorem 2.7

For $a \neq \pm 1$, let $s \in \mathbb{N}$ be such that $(s,t) = 1$. Then,

$$G_p(a) \cong G_p(-a) \cong G_p(a^s).$$

Proof

By lemma 2.3, $G_p(a) = \langle x, z, w \rangle$. Clearly, $G_p(a) = \langle x^{-1}, z, w \rangle$. Letting $y = x^{-1}$ and applying Tietze transformations, the defining relations in (2.4) become:

$$w^2 = z^t = (wy^{-1})^3 = y^{-p} = (wz)^2 = (y^{-a}zw)^3 = 1, \; y^{-a^2}z = zy^{-1}.$$

Since $w^2 = 1$, then

$$(wy^{-1})^3 = 1 \Leftrightarrow (wy)^3 = 1.$$

Also,

$$y^{-p} = 1 \Leftrightarrow y^p = 1.$$

$$y^{-a^2}z = zy^{-1} \Leftrightarrow y^{a^2}z = zy.$$

Hence the defining relations become:

$$w^2 = z^t = (wy)^3 = y^p = (wz)^2 = (y^{-a}zw)^3 = 1, \; y^{a^2}z = zy.$$

As $a^{2t} = 1$, then $(-a)^{2t} = ((-a)^2)^t = 1$. Now these are precisely

the defining relations of $G_p(-a)$, proving the first part.

Since $(s,t) = 1$, $\exists\, r,k \in \mathbb{Z}$ such that $rs - kt = 1$. We note that $rs \equiv 1 \pmod{t}$. In (2.4), let

$$y = z^s. \tag{2.5}$$

Then $$y^t = z^{st} = 1. \tag{2.6}$$

Also, $$w\,z\,w = z^{-1} \Rightarrow w\,z^s\,w = z^{-s}$$

$$\Rightarrow (wy)^2 = 1 \tag{2.7}$$

As $z^s \times z^{-s} = x^{a^{2s}}$, then

$$y \times y^{-1} = x^{a^{2s}}. \tag{2.8}$$

$$y^r = z^{sr} = z^{1+kt} = z \tag{2.9}$$

The relations (2.5)-(2.9) hold in (2.4), and so we can add them on. (2.9) allows us to eliminate z. On doing this, the defining relations become:

$$w^2 = (xw)^3 = y^t = (wy)^2 = x^p = 1,\ yxy^{-1} = x^{a^{2s}}. \tag{2.10}$$

$$y = y^{rs},\ y^{rt} = 1. \tag{2.11}$$

$$(wy^r)^2 = 1,\ x^{a^2} y^r = y^r x \tag{2.12}$$

$$(x^a y^r w)^3 = 1. \tag{2.13}$$

The relations (2.11) are clearly redundant and can be removed.

$$w\,y\,w = y^{-1} \Rightarrow w\,y^r\,w = y^{-r} \Rightarrow (wy^r)^2 = 1$$

Also,

$$y \times y^{-1} = x^{a^{2s}} \Rightarrow y^r \times y^{-r} = x^{a^{2rs}} = x^{a^{2+2kt}} = x^{a^2}.$$

Therefore the relations in (2.12) are redundant since they are implied by the other relations.

If <u>r is odd</u>, then let $q = (r-1)/2$.

$$(x^a y^r w)^3 = 1 \Leftrightarrow (y^{-q} x^a y^r w y^q)^3 = 1.$$

Since $yxy^{-1} = x^{a^{2s}}$, then $y^{-1}xy = x^{a^{-2s}}$, and $y^{-n}xy^n = x^{a^{-2ns}}$.

When $n = q$, $a^{2sn} = a^{sr-s} = a^{1+tk-s}$. Hence $y^{-q} x^a y^q = x^{a^{s-tk}}$.

So,

$$(x^a y^r w)^3 = 1 \Leftrightarrow (x^{a^{s-tk}} y w)^3 = 1 \text{ (using } wy^q w = y^{-q}).$$

Now,

$$x^{a^{s-tk}} = x^{a^s a^{-tk}} = x^{\pm a^s}.$$

In either case, the relations we are left with are those defining $G_p(a^s)$ or $G_p(-a^s)$ which are isomorphic. So for r odd,

$$G_p(a) \equiv G_p(a^s).$$

If r is even, then t is odd since $(r,t) = 1$. Also t-r is odd.

Let $u = (t-r+1)/2$. Then,

$$(x^a y^r w)^3 = 1 \Leftrightarrow (y^u x^a y^r w y^{-u}) = 1$$

$$\Leftrightarrow (x^{a^{u'}} y^{t+1} w)^3 = 1 \qquad (2.14)$$

where $u' = (t-r+1)s + 1 = ts + s - sr + 1 = t(s-k) + s$.

But $a^{u'} = a^{t(s-k)+s} = a^{t(s-k)} a^s = a^s$ or $-a^s \pmod p$. Again (2.14) reduces to

$$(x^{a^s} y w)^3 = 1 \text{ or } (x^{-a^s} y w)^3 = 1.$$

As above, in the case for r odd, we have

$$G_p(a) \equiv G_p(a^s).$$

Theorem 2.8

For $a \neq \pm 1$, $G_p(a)$ is isomorphic with

$$\langle x, w \mid x^p = w^2 = (wx)^3 = (x^{2a} w x^{a^{-1}} w)^2 = (x^a w x^{a^{-1}} w)^3 = 1 \rangle.$$

Proof

We use the presentation (2.4). As $wzw^{-1} = wzw = z^{-1}$, we have $wz^s w = z^{-s}$.

Also, by lemma 1.32, $z^s x z^{-s} = x^{a^{2s}}$. Using these we obtain the following:

$$z^s xwxwxwz^{-s} = 1 \text{ (since } (wx)^3 = 1).$$

$$x^{a^{2s}} w\, x^{a^{-2s}} w\, x^{a^{2s}} w = z^{2s} \tag{2.15}$$

$(x^a z w)^3 = 1$ implies

$$x^a z w x^a z w x^a w z^{-1} = 1$$

$$\Rightarrow x^a w x^{a^{-1}} w x^a w = z \tag{2.16}$$

Conjugating by z^s yields

$$z^s x^a w x^{a^{-1}} w x^a w z^{-s} = z$$

$$x^{a^{2s+1}} w\, x^{a^{-1-2s}} w\, x^{a^{1+2s}} w = z^{2s+1} \tag{2.17}$$

(2.15) and (2.17) can be combined into the one expression

$$z^r = x^{a^r} w\, x^{a^{-r}} w\, x^{a^r} w.$$

In particular, let $t = r$. Then,

$$z^t = x^{a^t} w\, x^{a^{-t}} w\, x^{a^t} w. \tag{2.18}$$

Now $a^t = 1$ or -1 since $a^{2t} = 1$. In either case, the word on the right hand side of (2.18) is $(xw)^3$ or $(x^{-1}w)^3$ and so is trivial. This shows that $z^t = 1$. Since it is implied by the other relations it can be omitted. We can replace the relation

$$zx = x^{a^2} z$$

by

$$zx^{-a^{-1}} = x^{-a} z \qquad (\text{since } x^p = 1).$$

(2.16) shows that we can eliminate z. On doing this our relations become:

$$x^p = w^2 = (wx)^3 = (x^{2a} w\, x^{a^{-1}} w)^2 = 1$$

$$(x^{3a} w\, x^{a^{-1}} w)^3 = 1 \tag{2.19}$$

$$w\, x^{a^{-1}} w\, x^a w\, x^{-a^{-1}} w\, x^{-a} w\, x^{-a^{-1}} w = x^{-a}. \tag{2.20}$$

But,

$$(x^{3a} w\, x^{a^{-1}} w)^3 = 1 \Leftrightarrow (x^{-a} w\, x^{-a^{-1}} w\, x^{-2a})^3 = 1$$

$$\Leftrightarrow (x^{a}w\ x^{a^{-1}}w)^{3} = 1 \qquad (2.21)$$

We replace (2.19) by (2.21). The relation (2.20) is now redundant for

$$x^{a}w\ x^{a^{-1}}w\ x^{a}w\ x^{-a^{-1}}w\ x^{-a}w\ x^{-a^{-1}}w$$

$$= x^{-a}w\ x^{-a^{-1}}w\ x^{-a}w\ x^{-a^{-1}}w\ x^{-a}w\ x^{-a^{-1}}w = 1.$$

We have now shown that for $p \neq 3$, $a \neq \pm 1$, that $G_p(a)$ is isomorphic with

$$\langle\ x, w \mid w^2 = x^p = (wx)^3 = (x^{2a}w\ x^{a^{-1}}w)^2 = (x^{a}w\ x^{a^{-1}}w)^3 = 1\ \rangle.$$

Corollary 2.9

$G_p(a)$, $a \neq \pm 1$, is isomorphic with

$$\langle\ x, w \mid w^2 = x^p = (wx)^3 = (x^{2a}w\ x^{a^{-1}}w)^2 = (x^{a}w\ x^{2a^{-1}}w)^2 = 1\ \rangle.$$

Proof

From the presentation in theorem 2.8, letting $y = x$ and $z = wxw$, we see that y and z satisfy

$$y^p = z^p = (y^{a^{-1}}z^{2a})^2 = 1.$$

Therefore, by lemma 1.30, we have

$$(y^{2a^{-1}}z^{a})^2 = 1 \Leftrightarrow (y^{a^{-1}}z^{a})^3 = 1.$$

That is,

$$(x^{2a^{-1}}w\ x^{a}w)^2 = 1 \Leftrightarrow (x^{a^{-1}}w\ x^{a}w)^3 = 1.$$

But $(x^{a^{-1}}w\ x^{a}w)^3 = 1$ in $G_p(a)$, by theorem 2.8. Therefore, we can replace this relation by

$$(x^{2a^{-1}}w\ x^{a}w)^2 = 1.$$

So far, we have only been able to classify two types of $G_p(a)$. Those for which $a = \pm 1$, and for which a is primitive in $GF(p)$. However, the next result does provide us with something new.

Theorem 2.10

For $p > 3$, the groups $G_p(2)$, $G_p(-2)$, $G_p\left(\frac{p+1}{2}\right)$, $G_p\left(\frac{p-1}{2}\right)$ are PSL(2,p). For $p > 5$, the groups $G_p(4)$, $G_p(-4)$, $G_p(1/4)$, $G_p(-1/4)$ are PSL(2,p), where by 1/4 we mean the element $b \in GF(p)$ such that $b.4 \equiv 1 \pmod p$.

Proof

From corollary 2.9,

$$G_p(2) = \langle\ x, w \mid w^2 = x^p = (wx)^3 = (x^4 w\, x^{1/2} w)^2 = (x^2 wxw)^2 = 1\ \rangle$$

when $p > 3$.

Now, $x^2wxwx^2wxw = x.xwxwx.xwxw = xwxwxw = 1$, and so this relation is redundant since it is implied by the others. What we are left with is precisely Sunday's presentation for PSL(2,p) [17]. Hence, $G_p(2)$ is PSL(2,p). By theorem 2.7, $G_p(-2)$ is PSL(2,p) also. Let s be such that $2^s \equiv 1 \pmod p$. Then $(p+1)/2 \equiv 2^{s-1} \pmod p$, and as $(s-1,s) = 1$, it follows from theorem 2.7 that $G_p\left(\frac{p+1}{2}\right)$ and $G_p\left(\frac{p-1}{2}\right)$ are also PSL(2,p).

For $p > 5$, by corollary 2.9,

$$G_p(4) = \langle\ x, w \mid w^2 = x^p = (wx)^3 = (x^8 wx^{1/4} w)^2 = (x^4 wx^{(p+1)/2} w)^2 = 1\rangle$$

where

$$1/4 = \begin{cases} \frac{p+1}{4} & \text{if } p \equiv -1 \pmod 4 \\ \\ \frac{3p+1}{4} & \text{if } p \equiv 1 \pmod 4 \end{cases} .$$

But by Sunday's results, the relations

$$w^2 = x^p = (wx)^3 = (x^4 wx^{(p+1)/2} w)^2 = 1$$

are sufficient to define PSL(2,p). So by Von Dyck's theorem, $G_p(4)$ is a homomorphic image of PSL(2,p). By corollary 2.6, for $p > 5$, $G_p(4)$ is non trivial, and so must be PSL(2,p). The rest of

the statement follows from theorem 2.7.

Remark

It is worth noting that for p = 5, a = 4, the presentation in corollary 2.9 still gives a presentation for PSL(2,5). It is rather unfortunate that $G_p(a)$ is not isomorphic with the above presentation for a = ±1.

We now obtain conditions which will tell us when $G_p(a)$ is PSL(2,p). For this, we use the presentation (2.4).

Lemma 2.11 Here z is as in 2.4.

Let α be a primitive element of GF(p) and H be the subgroup of $G_p(a)$ generated by x and z. If

$$(x^{2\alpha}wx^{\alpha^{-1}}w)^2,\ (x^{2\alpha^{-1}}wx^{\alpha}w)^2 \in H$$

then $G_p(a)$ is isomorphic with PSL(2,p).

Proof

Let K be the homomorphic image of $G_p(a)$ obtained by adding the relations

$$(x^{2\alpha}wx^{\alpha^{-1}}w)^2 = (x^{2\alpha^{-1}}wx^{\alpha}w)^2 = 1 \qquad (2.22)$$

The relations (2.22) together with $x^p = (wx)^3 = w^2 = 1$ define PSL(2,p) using corollary 2.9 and lemma 2.2. So K is either trivial or PSL(2,p). K is not trivial because the map from {x, w, z} into PSL(2,p) given by

$$x \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad w \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad z \mapsto \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$

extends to an epimorphism $K \longrightarrow PSL(2,p)$ by the substitution test. This is because these matrices satisfy the defining relations of K. Hence K is PSL(2,p). Let $N \trianglelefteq G_p(a)$ be such that

$G_p(a)/N \equiv K$. The mapping ϕ: $H \longrightarrow NH/N$ defined by $h \mapsto hN$ is an epimorphism. But $|H| = |\langle x, z \rangle| = t.p$ and $|NH/N| = tp$ also. Therefore ϕ is an isomorphism. Since $NH/N \equiv H/N \cap H$, we deduce $H \cap N = 1$. By hypothesis, the relations (2.22) hold in $G_p(a)$ and so $G_p(a) \equiv K \equiv PSL(2,p)$.

Remark

Showing any cyclic permutation of these two words are elements of H will also work. For example, showing that

$$(wx^{2\alpha}wx^{\alpha^{-1}})^2 \text{ and } (wx^{\alpha}wx^{2\alpha^{-1}})^2 \in H$$

will do.

Let us fix some $a \in GF(p)\backslash\{0, 1, -1\}$ and suppose a has order s in GF(p).

Definition 2.12

For any $f \in GF(p)$, we define

$$X_f = \{g \in GF(p);\ gf - 1 = \pm a^r,\ r = 1,2,\ldots,s\}$$

and

$$X_f^1 = \{\pm a^r;\ \pm a^r \in X_f\}$$

$$X_f^j = \{g \pm a^r;\ g \pm a^r \in X_f,\ g \in X_f^{j-1}\}$$

We shall say X_f is useful if for some integer n,

$$X_f = \bigcup_{i=1}^{n} X_f^i.$$

If s is odd, then $|X_f| = 2s$, while if s is even, $|X_f| = s$. As before we let t be the order of a^2 in GF(p). Therefore $|X_f| = 2t$.

Lemma 2.13

Let $a \in GF(p)\backslash\{0, 1, -1\}$ be of order s. Let t be the

order of a^2, so that $t = s$ or $2t = s$. There is always an element $\beta \in GF(p)$ such that X_β is useful with respect to powers of a.

Proof

There are three cases to consider.

(i) $s = t$. Choose $r \in \mathbb{N}$ satisfying $(r,s) = 1$ and let $\beta = 1+a^r$. We shall show X_β is useful. Clearly $1 \in X_\beta$. Let $h_1 = 1$, and $h_j = \frac{1-(-1)^j a^{rj}}{1+a^r}$. $h_j\beta - 1 = -(-1)^j a^{rj}$ which is a power of a or its negative. Hence $h_j \in X_\beta$. Also,

$$h_j = \frac{1 - (-1)^{j-1} a^{r(j-1)}}{1 + a^r} + (-1)^{j-1} a^{r(j-1)}$$

$$= h_{j-1} + (-1)^{j-1} a^{r(j-1)}.$$

Therefore, each element is obtained from a previously known element by adding or subtracting a power of a. The h_j series stops when

$$h_i = h_k \qquad \text{for some } i \text{ and } k.$$

Now $h_i - h_k = -(-1)^i a^{ri} \frac{(1 - (-1)^{k-i} a^{r(k-i)})}{1 + a^r}$

$$= -(-1)^i a^{ri} h_{k-i}.$$

Hence, $h_i = h_k$ when for some j, $h_j = 0$.

Now, $h_j = 0$ whenever $1 = (-1)^j a^{rj}$. As no power of a is -1, we require j to be even, and as $(r,s) = 1$, we require $j = 2s$. Therefore, we have defined $2s$ elements of X_β and so all elements of X_β. It follows that X_β is useful.

(ii) $s = 2t$, t even. Again we choose $r \in \mathbb{N}$ satisfying $(r,s) = 1$, and let $\beta = 1 + a^r$. As above, the $h_j \in X_\beta$. $h_j = 0$ whenever $1 = (-1)^j a^{rj}$. Now $(-1)^t a^{rt} = (-1)^r = -1$ since r is odd, and so $h_t \neq 0$. h_{2t} is zero since $1 = (-1)^{2t} a^{2rt}$. Again, we have

defined 2t elements of X_β, and the argument used in case (i) shows X_β useful.

(iii) $s = 2t$, t odd. Choose $r \in \mathbb{N}$ with $(r,s) = 1$. Let $\beta = 1-a^r$. Define $g_1 = 1$, and $g_j = \dfrac{1 - a^{rj}}{1 - a^r}$.

$$g_j = \frac{1 - a^{rj}}{1 - a^r} = \frac{1 - a^{r(j-1)}}{1 - a^r} + a^{r(j-1)} = g_{j-1} + a^{r(j-1)}.$$

Each $g_j \in X_\beta$ since $\beta g_j - 1 = -a^{rj}$. Also, the g_j series ends when $g_i = g_k$ for some i and k. Assume $i > k$.

$$g_i - g_k = \frac{-a^{ri} + a^{rk}}{1 - a^r} = a^{rk}\frac{(1 - a^{r(i-k)})}{1 - a^r} = a^{rk} g_{i-k}.$$

This is zero if, for some integer j, $g_j = 0$. Now, $g_j = 0$ whenever $a^{rj} = 1$. As $(r,s) = 1$, we require $j = s = 2t$. So, we have found all elements of X_β. As g_j is obtained from g_{j-1} by adding a power of a, it follows that X_β is useful. (This argument also works for case (ii)).

Corollary 2.14

With $\beta \in GF(p)$, suppose X_β is useful. If $\gamma = \beta a^r$ or $-\beta a^r$, then X_γ is useful.

Proof

If $\beta = f\gamma$ then $X_\gamma = f X_\beta$, for if $g \in X_\beta$, then $g\beta - 1$ is a power of a or its negative.

So, $(f^{-1}\beta)(fg) - 1 = \gamma(fg) - 1$ is also a power of a or its negative. Hence $fg \in X_\gamma$. In particular, when f is a power of a, then X_γ is useful by definition.

Definition 2.15

Given $a \in GF(p)\setminus\{0, 1, -1\}$, we shall say a is subprimitive

if, for any primitive element $\alpha \in GF(p)$, one of the pair of sets $(X_\alpha, X_{2\alpha})$, $(X_\alpha, X_{1/\alpha})$, $(X_{2\alpha}, X_{2/\alpha})$, $(X_{1/\alpha}, X_{2/\alpha})$ is such that both entries are useful with respect to powers of a.

This condition on the element a gives us the following result.

Theorem 2.16

If a is subprimitive, then $G_p(a)$ is PSL(2,p).

Proof

The defining relations of $G_p(a)$, using (2.4), are:

$$x^p = w^2 = (wx)^3 = (wz)^2 = z^t = (x^a zw)^3 = 1, \quad x^{a^2} z = zx.$$

Let $H = \langle x,z \rangle$. From lemma 2.11, it is sufficient to show

$$(x^{2\alpha} w\, x^{\alpha^{-1}} w)^2, \quad (x^{2\alpha^{-1}} w\, x^{\alpha} w)^2 \in H.$$

We consider the cosets of H.

$$Hx = Hz = H.$$

Define new cosets Hwx^f. Since $x^p = 1$, we can think of f as an element of GF(p).

$$Hwx^f x = Hwx^{f+1}$$

$$Hwx^f z = Hwz^{-1} x^f z = Hwx^{fa^{-2}}.$$

x and z just permute these cosets.

$$Hwxw = Hx^{-1}wx^{-1} = Hwx^{-1}.$$

Using lemma 1.32, we obtain

$$\begin{aligned} Hwx^{a^{2j}} w &= Hwz^j x z^{-j} w \\ &= Hz^{-j} wxwz^j \quad (\text{since } wzw = z^{-1}) \\ &= Hwxwz^j \\ &= Hwx^{-1} z^j. \end{aligned}$$

$$Hwx^{a^{2j}}w = Hwx^{-a^{-2j}} \tag{2.23}$$

$$Hwx^{a}w = Hz^{-1}x^{-a}wz^{-1}x^{-a}z \quad \text{(using } (x^{a}zw)^{3} = 1\text{)}$$

$$= Hwz^{-1}x^{-a}z$$

$$= Hwz^{-1}x^{-a^{-1}} = Hwx^{-a^{-1}}.$$

Again, using lemma 1.32, we get:

$$Hwx^{a^{2j+1}}w = Hwz^{j}x^{a}z^{-j}w$$

$$= Hwx^{a}wz^{j}$$

$$= Hwx^{-a^{-2j-1}}. \tag{2.24}$$

(2.23) and (2.24) can be combined into the single expression

$$Hwx^{a^{r}}w = Hwx^{-a^{-r}} \tag{2.25}$$

which implies,

$$Hwx^{-a^{r}}w = Hwx^{a^{-r}}.$$

Therefore we obtain no new cosets of the form $Hwx^{f}w$ provided $f \neq \pm a^{r}$. Define new cosets

$$Hwx^{f}wx^{g} \qquad (f \neq \pm a^{r}).$$

Again we can think of f and g as elements of GF(p), since $x^{p} = 1$.

$$Hwx^{f}wx^{g}.x = Hwx^{f}wx^{g+1},$$

$$Hwx^{f}wx^{g}.z = Hwx^{f}wzx^{ga^{-2}} = Hwx^{f}z^{-1}wx^{ga^{-2}}$$

$$= Hwx^{fa^{2}}wx^{ga^{-2}}$$

shows that x and z merely permute these cosets.

We now consider the action of w on these cosets.

$$Hwx^{f}wxw = Hwx^{f}x^{-1}wx^{-1} = Hwx^{f-1}wx^{-1}.$$

$$Hwx^{f}wx^{a^{2j}}w = Hwx^{f}wz^{j}xz^{-j}w$$

$$= Hwx^{f}z^{-j}wxwz^{j}$$

$$= Hwx^{fa^{2j}}{}_{wxwz^j}$$

$$= Hwx^{fa^{2j}-1}{}_{wx^{-1}z^j}$$

$$= Hwx^{(fa^{2j}-1)a^{2j}}{}_{wx^{-a^{-2j}}}. \qquad (2.26)$$

$$Hwx^{f}{}_{wx^{a}w} = Hwx^{f}{}_{z^{-1}x^{-a}zwx^{-a}z}$$

$$= Hwx^{f-1/a}{}_{wx^{-a}z^{z}}$$

$$= Hwx^{fa^{2}-a}{}_{wx^{-a^{-1}}}$$

$$= Hwx^{(fa-1)a}{}_{wx^{-a^{-1}}}.$$

$$Hwx^{f}{}_{wx^{a^{2j+1}}}{}_{w} = Hwx^{f}{}_{wz^{j}x^{a}z^{-j}w}$$

$$= Hwx^{f}{}_{z^{-j}wx^{a}wz^{j}}$$

$$= Hwx^{fa^{2j}}{}_{wx^{a}wz^{j}}$$

$$= Hwx^{(fa^{2j+1}-1)a}{}_{wx^{-a^{-1}}z^{j}}$$

$$= Hwx^{(fa^{2j+1}-1)a^{2j+1}}{}_{wx^{-a^{-2j-1}}} \qquad (2.27)$$

(2.26) and (2.27) combine into the single expression,

$$Hwx^{f}{}_{wx^{a^{r}}}{}_{w} = Hwx^{(fa^{r}-1)a^{r}}{}_{wx^{-a^{-r}}}$$

and similarly

$$Hwx^{f}{}_{wx^{-a^{r}}}{}_{w} = Hwx^{(-a^{r}f-1)(-a^{r})}{}_{wx^{a^{-r}}}.$$

We get no new cosets from

$$Hwx^{f}{}_{wx^{g}} \qquad \text{where } g = \pm a^{r}.$$

Suppose now that X_f is useful. Suppose further, that for some $g \in X_f$, we have shown

$$Hwx^{f}{}_{wx^{g}}{}_{w} = Hwx^{f'} \qquad (2.28)$$

where $f' = f/(1-fg)$.

Now, there is an $h \in X_f$ with $h = g + a^r$ or $h = g - a^r$. For convenience, take $h = g + a^r$. Then,

$$Hwx^{f}wx^{h}w = Hwx^{f}wx^{g+a^{r}}w$$

$$= Hwx^{f'}wx^{a^{r}}w \quad \text{where } f' = f/(1-fg)$$

$$= Hwx^{f''}wx^{-a^{-r}}$$

where

$$f'' = (f'a^{r} - 1)a^{r} = (fa^{r} - 1 + fg)a^{r}/(1-fg)$$

$$= \frac{(fh - 1)a^{r}}{1 - fg} .$$

Since $h,g \in X_{f}$, then f'' is a power of a or its negative. Hence,

$$Hwx^{f}wx^{h}w = Hwx^{f^{*}}$$

where

$$f^{*} = \frac{-1}{f''} - a^{-r} = -a^{-r}\left(1 + \frac{1-fg}{fh-1} \right)$$

$$= -a^{-r}\left(\frac{f(h-g)}{fh-1} \right)$$

$$= f/(1 - fh)$$

Similarly for $h = g - a^{r}$.

It follows that if we can show (2.28) holds for the powers of a in X_{f}, then for all $g \in X_{f}$, X_{f} useful,

$$Hwx^{f}wx^{g}w = Hwx^{f'}$$

where $f' = f/(1 - fg)$.

For $a^{r} \in X_{f}$ we have:

$$Hwx^{f}wx^{a^{r}}w = Hwx^{f'}wx^{-a^{-r}}$$

where $f' = (fa^{r} - 1)a^{r}$. But f' is a power of a or its negative since $a^{r} \in X_{f}$. Therefore,

$$Hwx^{f}wx^{a^{r}}w = Hwx^{f''}$$

where $f'' = -f'^{-1} - a^{-r} = -a^{-r}(1 + (fa^{r}-1)^{-1}) = f/(1 - fa^{r})$.

Similarly if $-a^r \in X_f$.

Now a is subprimitive. Without loss of generality, suppose X_α and $X_{1/\alpha}$ are useful. Now,

Now, $2\alpha^{-1}.\alpha - 1 = 1$ and so $2\alpha \in X_{1/\alpha}$ and $2\alpha^{-1} \in X_\alpha$. Therefore,

$$Hwx^{\alpha}wx^{2\alpha^{-1}}w = Hwx^{-\alpha}$$

and

$$Hwx^{\alpha^{-1}}wx^{2\alpha}w = Hwx^{-\alpha^{-1}}.$$

So, $wx^{\alpha}wx^{2\alpha^{-1}}wx^{\alpha}w$, $wx^{\alpha^{-1}}wx^{2\alpha}wx^{\alpha^{-1}}w \in H$.

Hence

$$(x^{2\alpha^{-1}}wx^{\alpha}w)^2,\ (x^{2\alpha}wx^{\alpha^{-1}}w)^2 \in H.$$

Therefore, by lemma 2.11, $G_p(a)$ is PSL(2,p).

Remarks

1. If a = 2, we need only show X_α useful, for by corollary 2.14, $X_{2\alpha}$ is useful.
2. If $2\alpha = \pm a^t$, again we only need X_α useful since

$$Hwx^{2\alpha}wx^{\alpha^{-1}}w = Hwx^{-2\alpha}$$

will hold as 2α is already a power of a. For,

$$Hwx^{2\alpha}wx^{\alpha^{-1}}w = Hwx^{-(2\alpha)^{-1}+\alpha^{-1}}w = Hwx^{(2\alpha)^{-1}}w = Hwx^{-2\alpha}$$

showing that

$$(x^{\alpha^{-1}}wx^{2\alpha}w)^2 \in H.$$

Corollary 2.17

Let $a \in GF(p)\setminus\{0, 1, -1\}$. If $G_p(b)$ is PSL(2,p), $b \in GF(p)$, and any one of the pairs $(X_b, X_{1/b})$, (X_b, X_{2b}), $(X_{2b}, X_{2/b})$ or $(X_{1/b}, X_{2/b})$ is such that both entries are useful with respect to powers of a, then $G_p(a)$ is PSL(2,p).

Proof

The proof is identical with the above once we have extended lemma 2.11, which is straightforward.

Example 2.18

Take p = 31. 3 is a primitive element of GF(31). By lemma 2.2, $G_{31}(3)$ is PSL(2,31). Theorem 2.7 shows that $G_{31}(a)$ is PSL(2,31) for a = 3, 9, 10, 11, 12, 13, 14, 17, 18, 19, 20, 21, 22, 23, 24, and 28.

Now $2^5 = 1 \pmod{31}$. As 3 - 1 = 2, it follows by lemma 2.13 (part (i)) that X_3 is useful. By corollary 2.14, X_6 is useful also. Therefore 2 is subprimitive. By theorem 2.7 and theorem 2.16, with a = 2, 4, 8, 16, 15, 23, 27, 29, we know $G_{31}(a)$ is PSL(2,31). $G_{31}(1)$ and $G_{31}(-1)$ are trivial. The only elements we are unsure about are

$$5,\ 6,\ 25 \text{ and } 26. \tag{2.29}$$

The elements in (2.29) form a subgroup of order six in GF(31)*, generated by 6. In fact, we always have 'trouble' with elements of order six.

For $a^6 \equiv 1 \pmod{p}$, the elements satisfying

$$\beta - 1 = -a^r \qquad r = 1,\ 5$$

are always powers of a. This is easily seen using the facts

$$1 + a^2 + a^4 \equiv 0 \pmod{p},$$

$$a^3 = -1,\ a^4 = -a,\ a^5 = -a^2.$$

So the only useful sets of this form are X_a and X_{a^5} and in general, a is not a primitive element of the field.

In the Behr-Mennicke paper [2], they say it would be desirable

to have a direct proof of their presentation. Theorem 2.16 provides a partial answer to that.

Theorem 2.19

If 2 or -2 is subprimitive in GF(p) then

$$G = \langle S,T \mid S^p = T^2 = (ST)^3 = (S^{\frac{p+1}{2}} TS^2T)^3 = 1 \rangle$$

is PSL(2,p).

Proof

Suppose 2 is subprimitive. For $p > 3$, by theorem 2.16, $G_p(2)$ is PSL(2,p). By theorem 2.7, $G_p(2)$ is isomorphic with $G_p(\frac{p+1}{2})$, which by theorem 2.8 is isomorphic with

$$\langle x,w \mid x^p = w^2 = (wx)^3 = (xwx^2w)^2 = (x^{\frac{p+1}{2}} wx^2w)^3 = 1 \rangle$$

The fourth relation is redundant since

$$xwx.xwxwx.xw = xwxwxw \quad \text{since } (xw)^3 = 1$$
$$= 1$$

is implied by the other relations, leaving us with the Behr-Mennicke presentation. The argument is similar for -2.

For p = 3, a simple coset enumeration shows that the index of $\langle S \rangle$ in G is 4, showing that G has order at most 12. G has PSL(2,3) as a homomorphic image using

$$S \longmapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad T \longmapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

and so is PSL(2,3).

One might be tempted to conjecture that, for $a \neq \pm 1$, $G_p(a)$ is PSL(2,p). However, this is not the case. Consider $12 \in GF(29)$. This has order 4, and the subgroup it generates in GF(29) is {12, -1, 17, 1}. By lemma 2.13, we know X_{18} is useful and that 18 is primitive in GF(29). However,

$$X_7 = \{0, 6, 15, 21\} \text{ and } X_{21} = \{0, 2, 5, 7\}$$

which are not useful. We cannot apply theorem 2.16. Using the presentation in (2.4), COSET is unable to determine the index of $\langle x,z \rangle$ in $G_{29}(12)$.

Let $H = \langle x, wx^2wx^{15}w \rangle$. Using COSET, we are able to show that $|G_{29}(12):H| = 30$. From RS and TTRANS, we obtained a presentation for H. On generators a and b, the defining relations are

$$(a\, b^2)^2 = 1$$

$$(a^3b^2a^{-1}b^{-1}a^{-1}b)^2 = 1$$

$$a^2b\ a^2b^{-1}a^2b^{-2}a^{-1}b\ a^2b^{-1}a^2b^{-1} = 1$$

$$a(a^2b^2a^{-1}b\ a\ b)^2a^{-1}(a^3b^2a^{-1}b^2)^3 = 1$$

$$(a^2b^2a^{-1}b\ a.b\ a^{-1}b^{-1}a\ b)^3a^{-1}b^{-1}a\ b = 1$$

Now $|H/H'|$ is obtained by performing elementary row operations on the relation matrix of the above presentation. The relation matrix is

$$\begin{pmatrix} 2 & 4 \\ 2 & 4 \\ 9 & -3 \\ 10 & 20 \\ 6 & 12 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 4 \\ 0 & 0 \\ 1 & -19 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 42 \\ 1 & -19 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Therefore, $|H/H'|$ is 42. This means that $G_{29}(12)$ is not PSL(2,29). To see this, suppose $G_{29}(12)$ is PSL(2,29). The relations of $G_{29}(12)$ are satisfied by

$$x \longmapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad w \longmapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad z \longmapsto \begin{pmatrix} 12 & 0 \\ 0 & 17 \end{pmatrix}$$

It is easy to check that $wx^2wx^{15}w$ corresponds to $\begin{pmatrix} -15 & 1 \\ 0 & -2 \end{pmatrix}$ which has order 14 in PSL(2,29). As $wx^2wx^{15}wx^2 = \begin{pmatrix} -15 & 0 \\ 0 & -2 \end{pmatrix}$ then H is the subgroup of upper triangular matrices of order 29.14. The derived group of H consists of matrices of the form:

$$\begin{pmatrix} a^{-1} & -b \\ 0 & a \end{pmatrix}\begin{pmatrix} c^{-1} & -d \\ 0 & c \end{pmatrix}\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} c & d \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

and so has order 29. Therefore $|H/H'|$ is 14 and not 42.

Another example is provided by taking $p = 89$, and $a = 34$, which has order four in GF(89). The subgroup

$$K = \langle x,\ wx^{3}wx^{30}w,\ wx^{9}wx^{10}w,\ wx^{-8}wx^{11}w,\ wx^{14}wx^{-19}w \rangle$$

has index 90 in $G_{89}(34)$. Using RS and TTRANS a presentation for K was obtained, and by abelianising this, we found $|K/K'| = 11.44$. So $G_{89}(34)$ is not PSL(2,89), for if it were, $|K/K'|$ would be 44.

These examples show the importance of having two of the sets

$$X_{\alpha},\ X_{2\alpha},\ X_{1/\alpha}$$

to be useful, where α is a primitive element of GF(p).

However, there is a counterexample to show that the conjecture

'$G_p(a) \equiv PSL(2,p) \Leftrightarrow$ a is subprimitive'

is false. For take $p = 19$ and $a = 8$. $8^{6} \equiv 1 \pmod{19}$. There are no elements $\beta \in GF(19)$, $\beta \neq a^{r}$, for which X_{β} is useful. Yet, using COSET, we can show that the order of $G_{19}(8)$ is 9.19.20, the order of PSL(2,19). In fact, this is the only counterexample we have been able to find.

Two questions arise from these examples and from theorem 2.10.

1. Is 2 subprimitive in GF(p) for any odd prime p?
2. If $G_p(a)$ is not PSL(2,p), $a \neq \pm 1$, is $G_p(a)$ finite or infinite?

A similar presentation to (2.1) for PSL(2,p) was given by Frasch [7] in 1933. His presentation was

$$\langle S, T, V \mid S^p = V^t = T^2 = (ST)^3 = (TV)^2 = 1, V^{-1}SV = S^{\alpha^2} \rangle \quad (2.31)$$

with the extra relation $(S^{\alpha}TV)^3 = 1$ when $p \equiv 1 \pmod 4$, $t = (p-1)/2$. The connection between (2.31) and (2.1) is a simple one, as can be seen by replacing V by U^{-1} in (2.31), and comparing it with (2.4). In chapter one, we have seen that PSL(2,p) is efficient if we can find a presentation on m generators and m+1 relations. Todd's presentation has deficiency -3 or -4 and we have shown, theorem 2.8, that this reduces to a deficiency -3 presentation for all primes p, p greater than three.

A great breakthrough came when Behr and Mennicke found the following two generator, four relation presentation for PSL(2,p) [2]:

$$\langle S, T \mid S^p = T^2 = (ST)^3 = (S^2TS^{(p+1)/2}T)^3 = 1 \rangle \quad (2.32)$$

Using this, Zassenhaus [20] obtained an efficient presentation for PSL(2,p), $p > 3$. However, he required two presentations, one to cover the case of $p = 17$. It has been pointed out (see [7],p95) that his presentation fails for greater values of p, congruent to $3 \pmod{14}$, such as 31 and 59.

In 1972, Sunday [17], succeeded in obtaining a deficiency -1 presentation for PSL(2,p), for all primes p. The Sunday presentation is

$$\langle S, T \mid S^p = (S^4TS^{(p+1)/2}T)^2 = 1, T^2 = (ST)^3 \rangle$$

This presentation was deduced from (2.32).

A symmetric presentation for PSL(2,p) was given by Beetham [1] and is:

$$\langle x, y \mid x^p = y^p = (x^{\alpha}y^{\alpha^{-1}})^2 = 1 \rangle \quad (2.33)$$

for all $\alpha \in GF(p)^*$. Beetham points out that there is no advantage

in trying to reduce (2.33) because of its symmetry, and because more economical presentations were known, [2],[20]. However,a rather nice presentation was obtained by Sidki [15] from the Behr-Mennicke presentation and is

$$\langle x, y \mid x^p = y^p = (xy)^2 = (x^{1/2}y^2)^2 = (x^{1/4}y^4)^2 = 1 \rangle \quad (2.34)$$

This shows that only three of Beetham's relations of the type

$$(x^{\alpha}y^{1/\alpha})^2 = 1$$

are necessary. Campbell and Robertson [5] have obtained an efficient presentation for PSL(2,p) from (2.34). A presentation for PSL(2,p) similar to that in (2.34) can be deduced directly from a presentation given by Sunday [17], by applying the modified Todd-Coxeter algorithm.

Theorem 2.20

PSL(2,p) is isomorphic with

$$\langle x, y \mid x^p = (xy)^3 = (x^2y)^2 = (x^4y^{(p+1)/2})^2 = 1 \rangle$$

Proof

We apply the modified Todd-Coxeter algorithm to Sunday's presentation

$SY = \langle S, T \mid S^p = T^2 = (ST)^3 = (S^4TS^{(p+1)/2}T)^2 = 1 \rangle$

using {S, TST} as subgroup generators. We set up the subgroup generator tables and relation tables.

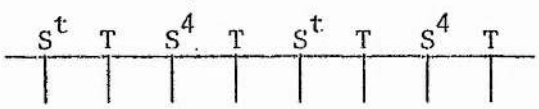
S	
1	1

T	S	T	
1	2	2	1

S	T	S	T	S	T	
1	1	2	2	1	1	1

T	T	
1	2	1

	p		
S	S	...	S
1			1



where $t = \frac{p+1}{2}$

Let S = x and T S T = y. From the first subgroup generator table, we have 1.S = x.1. Define 1 T = 1.2. From the second relation table we have completed the first line, showing 2T = 1.1. The second subgroup generator table now completes showing that

$$2\ S = y.2$$

The first relation table completes with the new information that

$$1\ T = h.1$$

where h is some word in x and y to be found.

$$1\ S\ T\ S\ T\ S\ T = 1$$

$$\text{i.e.} \quad x\ y\ x.h.1 = 1$$

$$\text{and so} \quad h = x^{-1}y^{-1}x^{-1}.$$

But $1\ T = 1.2 = x^{-1}y^{-1}x^{-1}.1$ giving rise to a coincidence. Hence

$$2 = x^{-1}y^{-1}x^{-1}.1\ .$$

The coset enumeration now terminates trivially showing that $SY = \langle S, T\ S\ T \rangle$ and

$$1\ S = x.1 \qquad 1\ T = x^{-1}y^{-1}x^{-1}.1\ ,$$

The new defining relations are

$$x^p = x^{-1}y^{-1}x^{-2}y^{-1}x^{-1} = 1$$

$$(x\ x^{-1}y^{-1}x^{-1})^3 = 1$$

$$(x^t.x^{-1}y^{-1}x^{-1}.x^4x^{-1}y^{-1}x^{-1})^2 = 1$$

where $t = \frac{p+1}{2}$.

That is

$$x^p = (x^2y)^2 = (x\ y)^3 = (x^t y\ x^4y^{-1})^2 = 1$$

Now

$$x\ y\ x = y^{-1}x^{-1}y^{-1}$$

$$\Rightarrow y^{-1}x^{-1}y^{-1} = x^{-1}y^{-1}x^{-1}$$

$$\Rightarrow x\ y^{-1}x^{-1} = y^{-1}x^{-1}y\ .$$

Using this we see that:

$$(x^t y\, x^4 y^{-1})^2 = 1 \Leftrightarrow (y^{-1}x^t y\, x^4)^2 = 1$$

$$\Leftrightarrow (x\, y^t x^{-1} x^4)^2 = 1$$

$$\Leftrightarrow (y^t x^4)^2 = 1$$

Theorem 2.21

PSL(2,p) is efficient and an efficient presentation is

$$\langle x, y \mid x^p = (y^t x^4)^2 = 1,\ (x^2 y)^2 = (x\, y)^3 \rangle$$

$$\equiv \langle x, y \mid x^p = (y^t x^4)^2 = 1,\ x\, y\, x = y\, x\, y \rangle \quad \text{where } t = \frac{p+1}{2}$$

Proof

First of all, that these groups are isomorphic follows from

$$(x^2 y)^2 = (x\, y)^3$$

$$\Leftrightarrow x\, y\, x^2 y = y\, x\, y\, x\, y$$

$$\Leftrightarrow x\, y\, x = y\, x\, y$$

Let G be the group presented above and $A = \langle (x^2 y)^2 \rangle$. $(x^2 y)^2$ commutes with $x^2 y$ and xy. It also commutes with x and y since

$$x = x^2 y . y^{-1} x^{-1}$$

and

$$y = x^{-1} . x\, y$$

Therefore $A \leq Z(G)$. For $p \neq 3$, G is perfect. To see this we perform elementary row operations on the relation matrix

$$\begin{pmatrix} p & 0 \\ 8 & p+1 \\ 1 & -1 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & p \\ 8 & p+1 \\ 1 & -1 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & p \\ 8 & 1 \\ 1 & -1 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & p \\ 0 & 9 \\ 1 & -1 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & -1 \end{pmatrix}.$$

since (p,3) = 1, and so $A \leq G'$. For p = 3, the defining relations for G/G' reduce to

$$x^3 = y^4 x^2 = 1,\ x = y$$

Hence $y\, x^2 = 1$ and so $y\, x^2 \in G'$. Again, $A \leq G'$. By theorem 2.20, G/A = PSL(2,p). G is therefore a stem extension of PSL(2,p) and so is either PSL(2,p) or SL(2,p) by theorem 1.19. Since $Z(SL(2,p)) = C_2$

then we have

$$(x^2y)^2 = 1 \quad \text{or} \quad (x^2y)^4 = 1.$$

Similarly, $(x\ y)^3$ is central in G and $(x\ y)^3 = 1$ or $(x\ y)^6 = 1$. In either case, $(xy)^6 = 1$ holds in G.

Now $x\ y\ x = y\ x\ y$

$$\Rightarrow y^{-1}x\ y = x\ y\ x^{-1}$$

Raising this to the power p gives $y^p = 1$. With $t = \frac{p+1}{2}$, we have

$$\begin{aligned} x^2y^tx^2 &= x^{-2}y^{-t}x^{-2} \\ &= x^{-2.3}x^4y^{-t}x^{-2} \\ &= x^{-2.3}y^{-t}x^{-4}y^{-1}x^{-2} \\ &= x^{-2.3}y^{-t}.x^{-4}.x^2y.(x\ y)^3 \end{aligned}$$

since $(x^2y) = (xy)^3y^{-1}x^{-2}$.

$$x^2y^tx^2 = x^{-2.3}y^{-t}x^{-2}y(xy)^3$$

As in the proof of lemma 1.30, and using the fact that $(x\ y)^3$ is central, this generalises to

$$x^2y^tx^2 = x^{-(2k+1)2}.y^{-t}x^{-2}y^k(xy)^{3k} \qquad k \in \mathbb{N}.$$

With $k = \frac{p-1}{2} = t-1$, we have

$$x^2y^tx^2 = y^{-t}x^{-2}y^{-t}(xy)^{3(t-1)} \quad \text{since} \quad y^{t-1} = y^{p-t} = y^{-t}$$

giving

$$(y^tx^2)^3 = (xy)^{3(t-1)}.$$

There are two cases to consider.

(i) t odd. Then $(y^tx^2)^3 = 1$ since $(xy)^6 = 1$.

$$\begin{aligned} y^tx^2y^t &= x^{-2}.y^{-t}x^{-2} \\ &= x^{-2}.x^4y^tx^4x^{-2} \end{aligned}$$

So, $$y\ x^2y = y^tx^2y^tx^2y^t = x^{-2}$$

$$(y\ x^2)^2 = 1 \quad \text{showing that G is PSL(2,p).}$$

(ii) t even, then $(y^t x^2)^3 = (xy)^3$.

$$\begin{aligned} y^t x^2 y^t &= (xy)^3 x^{-2} y^{-t} x^{-2} \\ &= (xy)^3 x^{-2} x^4 y^t x^4 x^{-2} \\ &= (xy)^3 x^2 y^t x^2. \end{aligned}$$

Hence,

$$\begin{aligned} y\, x^2 y &= y^t (xy)^3 x^2 y^t x^2 y^t \\ &= (xy)^3 y^t x^2 y^t x^2 y^t \qquad \text{(since } (xy)^3 \text{ is central)} \\ &= (xy)^6 x^{-2} \\ &= x^{-2} \qquad \text{(since } (xy)^6 = 1). \end{aligned}$$

Therefore, $(yx^2)^2 = 1$ and so G is PSL(2,p).

This presentation is identical to one found by J.H. Renshaw (see [13]).

Definition 2.22

The special linear group over the ring of integers $\mathbb{Z}(m)$, $SL(2,\mathbb{Z}(m))$, is the group of 2x2 matrices with determinant 1 with entries in $\mathbb{Z}(m)$. In keeping with definition 1.7, we define the projective special linear group over $\mathbb{Z}(m)$ to be,

$$PSL(2,\mathbb{Z}(m)) = \frac{SL(2,\mathbb{Z}(m))}{Z(SL(2,\mathbb{Z}(m)))}.$$

In [2], Behr and Mennicke give the following presentation for $SL(2,\mathbb{Z}(m))$

$$\langle A,B \mid A^m = B^4 = (A^2 B A^{(m+1)/2} B)^3 = 1,\ (AB)^3 = B^2 \rangle \quad (2.35)$$

where m is an odd integer.

Using this presentation, Sunday [17] deduces the following presentation for $SL(2,\mathbb{Z}(m))$, m odd.

$$\langle S, T \mid S^m = T^2 = (ST)^3 = (S^4 T S^{(m+1)/2} T)^2,\ T^4 = 1 \rangle \qquad (2.36)$$

He states that by adding $T^2 = 1$ to (2.36) we obtain PSL(2,$\mathbb{Z}$(m)), and he finds a two generator, three relation presentation for PSL(2,$\mathbb{Z}$(m)). Unfortunately, our definition and Sunday's definition of PSL(2,$\mathbb{Z}$(m)) are different unless m is prime or of prime power. We shall verify these remarks and go on to find an efficient presentation for PSL(2,$\mathbb{Z}$(m)) when m is odd.

J. Mennicke in [11] shows that the multiplicator of SL(2,$\mathbb{Z}$(p^r)) is trivial, for any prime p. Rudolph Beyl (private communication) has found flaws in this argument when p = 2, although the case of p odd seems to be correct. The Schur Multiplicator plays an important part in what follows, and so to avoid any dilemmas we shall keep to m odd.

In order to find an efficient presentation for PSL(2,$\mathbb{Z}$(m)), we shall find a deficiency zero presentation for SL(2,$\mathbb{Z}$(m)) and then factor out by its centre.

Let

$$m = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$$

be the prime decomposition of m, where each p_i is an odd prime. It is well known that

$$\mathbb{Z}(m) = \mathbb{Z}(p_1^{a_1}) \times \mathbb{Z}(p_2^{a_2}) \times \ldots \times \mathbb{Z}(p_r^{a_r})$$

(see for example [6], p33).

Hence every $x \in \mathbb{Z}(m)$ has a unique representation as the r-tuple $(x_1, x_2, \ldots, x_r)$, where each x_i satisfies

$$x_i \equiv x \pmod{p_i^{a_i}} \qquad i = 1,2,\ldots,r.$$

Lemma 2.23

The centre of $SL(2,\mathbb{Z}(m))$ consists of the matrices

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

where a satisfies $a^2 \equiv 1 \pmod{m}$.

Proof

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(SL(2,\mathbb{Z}(m)))$. By definition, central elements commute with all other elements, and so in particular with

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} .$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}$$

which implies $c = 0$, $a = d$.

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -b & a \\ -a & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 0 & a \\ -a & -b \end{pmatrix}$$

which implies $b = 0$.

That is, all central elements have the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ with

$a^2 = 1$.

Lemma 2.24

The equation $x^2 = 1$ has two solutions in $\mathbb{Z}(p^r)$, p an odd prime.

Proof

Certainly $x = \pm 1$ satisfy the above equation, and so there are at least two solutions. Now suppose that $x \neq \pm 1$ satisfies

$$x^2 \equiv 1 \pmod{p^r}.$$

Then, $(x-1)(x+1) \equiv 0 \pmod{p^r}$, and so $x-1$ and $x+1$ are zero divisors and are both divisible by p. For, if $yz \equiv 0 \pmod{p^r}$, $y,z \neq 0$,

suppose z is not divisible by p. Then $(z,p) = 1$ and $(z,p^r) = 1$. Hence, $\exists$ integers m,n with

$$mz + np^r = 1,$$

showing $mz \equiv 1 \pmod{p^r}$. That is, z is invertible in $\mathbb{Z}(p^r)$. Hence $yz \equiv 0 \Rightarrow y = 0$, giving a contradiction. A similar argument holds for y. As p divides x-1 and x+1, then

$$p \mid x+1-x+1 = 2.$$

But $p \nmid 2$ since $p \geq 3$. Hence there are only two solutions to the equation.

Remark

When $p = 2$, this lemma is false. For example, take $p^r = 16$. Then 1, 15, 7 and 9 satisfy $x^2 = 1$.

Corollary 2.25

With m as above, there are 2^r solutions to the equation

$$x^2 = 1 \pmod{m}.$$

Proof

For each $p_i^{a_i}$, there are only two solutions to the equation. Hence the r-tuples $(e_1, e_2, \ldots, e_r)$, where $e_i = 1$ or -1, satisfy $x^2 = 1 \pmod{m}$, and there are 2^r such r-tuples.

Corollary 2.26

With m as above,

$$|Z(SL(2,\mathbb{Z}(m)))| = 2^r.$$

Lemma 2.27

With m as above,

$$M(SL(2,\mathbb{Z}(m))) = 1,$$

and $SL(2,\mathbb{Z}(m))$ is its own covering group.

Proof

From lemma 3.2 of [11], $M(SL(2,\mathbb{Z}(m))) = 1$, which is the result for $m = p_1^{a_1}$. For $r \geqslant 2$, we have by lemma 3.1 of [11] that $M(SL(2,\mathbb{Z}(m))) = 1$. It follows from the definition of a covering group and corollary 1.17 that $SL(2,\mathbb{Z}(m))$ is its own covering group.

Lemma 2.28

With m as above, $SL(2,\mathbb{Z}(m))$ is a stem extension of $PSL(2,\mathbb{Z}(m))$.

Proof

Let $H = SL(2,\mathbb{Z}(m))$. By definition 2.22,

$$H/Z(H) \equiv PSL(2,\mathbb{Z}(m)).$$

It remains for us to show that $Z(H) \leqslant H'$. If $(m,3) = 1$, it is easy to check using (2.35) that H is perfect and so $Z(H) \leqslant H' = H$. For $(m,3) = 3$, again using (2.35) we see that $H/H' \equiv C_3$. Suppose $Z(H) \not\leqslant H'$. Let $Z(H) \cap H' = A$. Since $|Z(H)| = 2^r$ then $|A| = 2^s$ for some $s < r$. Now $A \trianglelefteq H$. Let, $H/A = \overline{H}$, $H'/A = \overline{H}'$ and $Z(H)/A = \overline{Z}$. $\overline{H}' \cap \overline{Z} = 1$. Also as $\overline{Z} \subseteq Z(\overline{H})$ we have that

$$\overline{Z}\overline{H}' = \overline{H}'\overline{Z} = K \leqslant \overline{H}.$$

Now $\overline{H}' \leqslant K$ since $\overline{Z}$ is non-trivial. Since $\overline{H}/\overline{H}' \equiv C_3$, it is simple. It follows that $\overline{H}'$ is maximal in $\overline{H}$ and so $K = \overline{H}$. Therefore, $\overline{H} = \overline{H}' \times \overline{Z}$ which implies $\overline{Z} \equiv C_3$, which is impossible. Hence, $Z(H) \leqslant H'$.

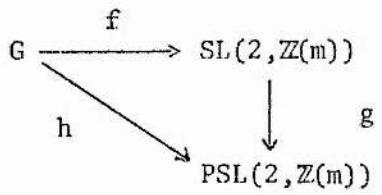
Theorem 2.29

$SL(2,\mathbb{Z}(m))$ is the unique covering group of $PSL(2,\mathbb{Z}(m))$. $M(PSL(2,\mathbb{Z}(m))) = (C_2)^r$.

Proof

Let G be the covering group of $PSL(2,\mathbb{Z}(m))$ such that G has

$SL(2,\mathbb{Z}(m))$ as a homomorphic image. This we can do by theorem 1.16. Also by the proof of theorem 1.16 the diagram



is commutative with f, g and h epimorphisms.

$SL(2,\mathbb{Z}(m)) \cong G/\text{Ker } f$. Now, $\exists B \leqslant G' \cap Z(G)$ with $G/B \cong PSL(2,\mathbb{Z}(m))$. Let $a \in \text{Ker } f$.

$$ah = afg = 1g = 1$$

and so $a \in \text{Ker } h = B$, Therefore $\text{Ker } f \subseteq B \leqslant G' \cap Z(G)$, and so G is a stem extension of $SL(2,\mathbb{Z}(m))$. Moreover,

$$|SL(2,\mathbb{Z}(m))| \leqslant |G| \leqslant |M(SL(2,\mathbb{Z}(m)))|\ |SL(2,\mathbb{Z}(m))| = |SL(2,\mathbb{Z}(m))|$$

since $M(SL(2,\mathbb{Z}(m))) = 1$.

Therefore $G = SL(2,\mathbb{Z}(m))$ and so $SL(2,\mathbb{Z}(m))$ is a covering group of $PSL(2,\mathbb{Z}(m))$. It follows from the definition of a covering group that

$$M(PSL(2,\mathbb{Z}(m))) = (C_2)^r.$$

Since $\left|\frac{PSL(2,\mathbb{Z}(m))}{PSL'(2,\mathbb{Z}(m))}\right| = 1$ or 3, then by corollary 1.17, $PSL(2,\mathbb{Z}(m))$ has a unique covering group.

We now verify the remarks we made about Sunday's presentation for $PSL(2,\mathbb{Z}(m))$. Recall that the number of defining relations for a group has to be at least

$$d(G) + d(M(G)).$$

For a two generator presentation for $PSL(2,\mathbb{Z}(m))$, by theorem 2.29, we require at least r+2 defining relations where

$$m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}.$$

Therefore, Sunday's results can only hold if m is a prime or of

prime power. We now proceed to find an efficient presentation for $PSL(2,\mathbb{Z}(m))$ on two generators and r+2 relations. The first step is to find a deficiency zero presentation for $SL(2,\mathbb{Z}(m))$.

Let G_o denote $SL(2,\mathbb{Z}(m))$ as presented in (2.36), and let G_1 be:

$$\langle S, T \mid S^m = T^2 = (ST)^3 = (S^{(m+1)/2}TS^4T)^2 = 1 \rangle$$

where m is an odd integer as above.

Theorem 2.30

$G_1 \cong \frac{SL(2,\mathbb{Z}(m))}{\langle \pm I \rangle}$ where I is the identity matrix, and $SL(2,\mathbb{Z}(m))$ is its unique covering group.

Proof

Let $A = \langle T^2 \rangle \leq G_o$. Since $T^2 = S^m$, T^2 commutes with S. T^2 clearly commutes with T and so $A \leq Z(G_o)$. In the proof of lemma 2.28, we showed that

$$Z(SL(2,\mathbb{Z}(m))) \leq SL'(2,\mathbb{Z}(m)).$$

Therefore, $A \leq Z(G_o) \cap G_o'$. As $G_o/A \cong G_1$, G_o is a stem extension of G_1. With the same argument used in theorem 2.29, G_1 replacing $PSL(2,\mathbb{Z}(m))$, it follows that

$$|M(G_1)| = |A| = 2.$$

Moreover, since G_1/G_1' is trivial or C_3, then by corollary 1.17, $SL(2,\mathbb{Z}(m))$ is the unique covering group of G_1.

Let G_2 be the group defined as

$$\langle S, T \mid S^m = T^2 = (ST)^3 = (S^{(m+1)/2}\, T\, S^4T)^2 \rangle$$

as defined by Sunday [17]. Let $C = \langle T^4 \rangle$. T^2 is central since it commutes with S and T, and so $C \leq Z(G_2)$. A presentation for G_2/G_2' is obtained by adding on $[S,T] = 1$.

$$G_2/G_2' = \langle S, T \mid S^m = T^2,\ S^3T = 1,\ S^9T^4 = [S,T] = 1 \rangle$$

$$= \langle S \mid S^m = S^3 = 1 \rangle .$$

So $T \in G_2' \Rightarrow T^4 \in G_2'$. Hence $C \leq Z(G_2) \cap G_2'$. Also, $G_2/C \equiv G_o$ and $G_o \equiv SL(2,\mathbb{Z}(m))$, showing that G_2 is a stem extension of $SL(2,\mathbb{Z}(m))$. By lemma 2.27, $G_2 \equiv SL(2,\mathbb{Z}(m))$. The relations of G_2 are satisfied by $S = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}$, $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ which generate $SL(2,\mathbb{Z}(m))$.

Adding $T^2 = 1$ to G_2 gives the presentation for G_1. But this is the same as letting $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Hence, $G_1 \equiv \dfrac{SL(2,\mathbb{Z}(m))}{\langle \pm I \rangle}$.

Obtaining a deficiency zero presentation for $SL(2,\mathbb{Z}(m))$ presents no problem. Campbell and Robertson [3] have produced a deficiency zero presentation for $SL(2,p)$, where p is an odd prime. The results in this paper generalize easily to this case. For completeness, we give the proofs of these results and keep to their notation.

Let $\tilde{G}_m$ be the group

$$\langle x, y \mid x^2 = (xy)^3 = 1,\ x\, y^4 x\, y^{(m+1)/2} x\, y^4 x\, y^{(3m+1)/2} = 1 \rangle .$$

Theorem 2.31

$$\tilde{G}_m \equiv G_1 .$$

Proof

We first show $\tilde{G}_m$ is a stem extension of G_1. If $(m,3) = 1$,

then $\tilde{G}_m$ is perfect, and so $y^m \in \tilde{G}'_m$. For $(m,3) = 3$, then $\tilde{G}_m/\tilde{G}'_m$ has the following presentation.

$$\langle x, y \mid [x,y] = y^6 = xy^3 = y^{3+2m} = 1 \rangle$$

Clearly $y^3 = 1$ since $3+2m$ is odd. Therefore, $y^3 \in \tilde{G}'_m$, which implies $y^m \in \tilde{G}'_m$.

$$y^{-m} = (xy^4xy^{(m+1)/2})^2$$

showing that

$$[y^m, xy^4x] = 1. \tag{2.37}$$

Consider

$$[y^m, y^4x\, y^{(m+1)/2}x\, y^4x\, y^{(3m+1)/2}x] = 1 \tag{2.38}$$

Case 1

If $\frac{m+1}{2} \equiv 0 \pmod 4$, then $\frac{3m+1}{2} \equiv -1 \pmod 4$. Since $x^2 = 1$,

then $$x\, y^{(m+1)/2}x = (x\, y^4x)^k \text{ for some } k \in \mathbb{Z}, \text{ while}$$

$$x\, y^{(3m+1)/2}x = x\, y^{-1}x^2y^{1+(3m+1)/2}x$$

$$= x\, y^{-1}x(x\, y^4x)^n \text{ for some } n \in \mathbb{Z}.$$

On applying (2.37), (2.38) becomes

$$[y^m, x\, y^{-1}x] = 1. \tag{2.39}$$

Case 2

If $\frac{m+1}{2} \equiv -1 \pmod 4$, then $\frac{3m+1}{2} \equiv 0 \pmod 4$. As in case 1, (2.38) reduces to $[y^m, x\, y^{-1}x] = 1$.

As $(xy)^3 = 1$ and $x^2 = 1$, then

$$x\, y^{-1}x = y\, x\, y. \tag{2.40}$$

Substituting into (2.39) we have

$$[y^m, y\, x\, y] = 1,$$

that is,

$$[y^m, x] = 1.$$

Hence $y^m \in Z(\tilde{G}_m)$ for case 1 and case 2.

Case 3 If

If $\frac{m+1}{2} \equiv 1 \pmod 4$ then $\frac{3m+1}{2} \equiv 2 \pmod 4$.

Then, $x\, y^{(m+1)/2} x = x\, y^{(m+1)/2-1} x\, x\, y\, x$

$= (x\, y^4 x)^k\, x\, y\, x$ for some $k \in \mathbb{Z}$.

Similarly we have

$$x\, y^{(3m+1)/2} x = x\, y^2 x (x\, y^4 x)^n \text{ for some } n \in \mathbb{Z}$$

(2.38) now reduces to

$$[y^m,\ x\, y\, x\, y^4 x\, y^2 x] = 1.$$

Case 4

Finally, if $\frac{m+1}{2} \equiv 2 \pmod 4$ then $\frac{3m+1}{2} \equiv 1 \pmod 4$. As in case 3,

(2.38) can be reduced to

$$[y^m,\ x\, y\, x\, y^4 x\, y^2 x] = 1. \qquad (2.41)$$

Using (2.40), (2.41) becomes:

$$[y^m,\ x\, y^3 x\, y^2 x] = 1$$

$$\Rightarrow [y^m,\ x\, y^{-1} x\, y^2 x] = 1 \qquad \text{(using (2.37))}$$

$$\Rightarrow [y^m,\ x\, y^3 x] = 1 \qquad \text{(using (2.40))}$$

$$\Rightarrow [y^m,\ x\, y^{-1} x] = 1 \qquad \text{(using (2.37))}$$

$$\Rightarrow [y^m,\ x] = 1\ . \qquad \text{(using (2.40) again)}$$

Hence, in all four cases, we have shown that $y^m \in \tilde{G}_m' \cap Z(\tilde{G}_m)$. Also, $\tilde{G}_m / \langle y^m \rangle \equiv G_1$, so $\tilde{G}_m$ is a stem extension of G_1. By theorem 2.30, it follows that $\tilde{G}_m$ is either $SL(2,\mathbb{Z}(m))$ or $\frac{SL(2,\mathbb{Z}(m))}{\langle \pm I \rangle}$.

If the latter is true, then $y^m = 1$ and so $y^{2m} = 1$. On the other hand, if $\tilde{G}_m$ is $SL(2,\mathbb{Z}(m))$, then as $y^m \in Z(SL(2,\mathbb{Z}(m)))$, y^m must be an element of order two. Hence the relation $y^{2m} = 1$, holds in $\tilde{G}_m$.

$$x\, y^{(m+1)/2} x\, y^4 x\, y^{(3m+1)/2} x\, y^4 = 1$$

$$\Rightarrow \quad x\, y^{(m+1)/2} x\, y^{4} x\, y^{(3m+1)/2} y^{-1-2m} x = y^{-4} x\, y^{-1} x \quad \text{since } y^{2m}=1$$

$$\Rightarrow \quad x\, y^{(m+1)/2} x\, y^{4} x\, y^{-(m+1)/2} x = y^{-4} x\, y^{-1} x \,. \qquad (2.42)$$

But,

$$y^{-4} x\, y^{-1} x = y^{-3} x\, y \quad \text{(using (2.40))}$$

$$= y^{-2}(y^{-1} x\, y^{-1}) y^{2}$$

$$= y^{-2}(x\, y\, x) y^{2} \quad \text{(using (2.40))}.$$

Substituting this into (2.42) gives,

$$x\, y^{(m+1)/2} x\, y^{4} x\, y^{-(m+1)/2} x = (y^{-2} x) y (x y^{2}).$$

Raising this to the power m gives $y^{m} = 1$. Hence $\tilde{G}_m = G_1$.

Theorem 2.32

With m as above, $SL(2,\mathbb{Z}(m))$ has the deficiency zero presentation

$$\langle x, y \mid x^2 = (xy)^3,\ (x\, y^4 x\, y^{(m+1)/2})^2 y^m x^{2k} = 1 \rangle$$

where

$$k = \begin{cases} m/3 & \text{if } m \equiv 0 \pmod 3 \\ (m-1)/3 & \text{if } m \equiv 1 \pmod 3 \\ (m-2)/3 & \text{if } m \equiv 2 \pmod 3 \end{cases}$$

Proof

Let H_m be the group defined in the statement of this theorem. x and xy generate H_m, and as x^2 commutes with xy, we have that x^2 is central. Moreover, $x \in H_m'$ for any m and so $x^2 \in H_m'$. By theorem 2.31, $H_m/\langle x^2 \rangle \equiv G_1$, and therefore H_m is a stem extension of G_1. However, as $M(G_1) = C_2$, G_1 cannot have a deficiency zero presentation. Therefore H_m is $SL(2,\mathbb{Z}(m))$.

What are the corresponding matrices for x and y? When k is odd,

we take

$$x \longmapsto A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad y \longmapsto B = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

and for k even we take

$$x \longmapsto C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad y \longmapsto D = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$$

To see that these do satisfy the above relations, we consider the two cases separately.

First of all, consider k odd. It is easy to check that

$$B^k = \begin{pmatrix} 1 & 0 \\ -k & 1 \end{pmatrix}.$$

so that $B^m = 1$. Now

Now $A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $AB = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$

$$(AB)^3 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$AB^4A\,B^{(m+1)/2} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -(m+1)/2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 4 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1/2 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{(where } 1/2 = (m+1)/2\text{)}$$

$$= \begin{pmatrix} 1 & -4 \\ 1/2 & -1 \end{pmatrix}$$

Hence,

$$(A\,B^4A\,B^{(m+1)/2})^2B^mA^{2k} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

We know that $SL(2,\mathbb{Z}(m)) = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix} \right\rangle$ (see [11],[17]).

Now $\begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = B^{-1}A^2$. Hence $\langle A, B \rangle = SL(2,\mathbb{Z}(m))$.

Secondly, consider k even.

$$C^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad CD = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$$

and $(CD)^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = C^2$.

$$D^k = \begin{pmatrix} (-1)^k & 0 \\ (-1)^{k+1}k & (-1)^k \end{pmatrix} \text{ and so } D^m = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

For $(m+1)/2$ even,

$$CD^4CD^{(m+1)/2} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -(m+1)/2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -4 \\ 1/2 & -1 \end{pmatrix}$$

while for $(m+1)/2$ odd,

$$CD^4CD^{(m+1)/2} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ (m+1)/2 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} -4 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} (m+1)/2 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 4 \\ -(m+1)/2 & 1 \end{pmatrix}.$$

In both cases,

$$(CD^4CD^{(m+1)/2})^2D^mC^{2k} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

C, D generate $SL(2,\mathbb{Z}(m))$ since $C^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $D^{-1} = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}$.

In order to find an efficient presentation for $PSL(2,\mathbb{Z}(m))$, we need to find r relations which will 'kill off' the centre of $SL(2,\mathbb{Z}(m))$. Let $a \in \mathbb{Z}(m)$ be such that $a^2 = 1 \pmod m$. It is easy to check that

$$(AB^a)^3 = \begin{pmatrix} -a & 0 \\ 0 & -a \end{pmatrix} \in Z(SL(2,\mathbb{Z}(m)) \text{ and } (CD^a)^3 = \begin{pmatrix} (-1)^a a & 0 \\ 0 & (-1)^a a \end{pmatrix}$$

$\in Z(SL(2,\mathbb{Z}(m))$.

Central elements therefore correspond to words of the form $(xy^a)^3$ in H_m.

Let $E = \{a \in \mathbb{Z}(m);\ a^2 \equiv 1 \pmod{m}\}$, $|E| = 2^r$. We know every $a \in E$ has a unique representation as the r-tuple $(e_1, e_2, \ldots, e_r)$ where $e_i = \pm 1$. Now, E under multiplication is a group isomorphic with $(C_2)^r$. Let V be the r-dimensional vector space over $\mathbb{Z}(2)$. There is an obvious isomorphism from $(E,\cdot)$ to $(V,+)$ given by

$$(b_1, b_2, \ldots, b_r) \longmapsto (\beta_1, \beta_2, \ldots, \beta_r)$$

where $$\beta_i = \begin{cases} 0 & \text{if } b_i = 1 \\ 1 & \text{if } b_i = -1 \end{cases}$$

The set of r-vectors $\{(1, 1, \ldots, 1), (0, 1, 1, \ldots, 1), (0, 0, 1, \ldots, 1) \ldots (0, 0, \ldots, 0, 1)\}$ form a basis for V. Likewise the set

$$B = \{(-1, -1, \ldots, -1), (1, -1, -1, \ldots, -1), (1, 1, -1, \ldots, -1), \ldots (1, 1, \ldots, 1, -1)\}$$
$$= \{d_i;\ i = 0,1,\ldots, r-1\}$$

is such that every $a \in E$ can be represented as a product of elements in B. For each $d_i \in B$ we add the relation

$$(x\, y^{-d_i})^3 = 1$$

to H_m. We have chosen B such that $-1 \in B$ and so we will add the relation $(x\, y)^3 = 1$ to H_m. This gives a 2 generator, r + 2 relation presentation. In order to exhibit that this is $PSL(2,\mathbb{Z}(m))$ we need to show that there are no central elements. Now any $b \in E$ can be written as

$$b = d_{i_1} d_{i_2} \ldots d_{i_s} \quad \text{where } d_{i_j} \in B.$$

and so $\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} d_{i_1} & 0 \\ 0 & d_{i_1} \end{pmatrix} \begin{pmatrix} d_{i_2} & 0 \\ 0 & d_{i_2} \end{pmatrix} \ldots \begin{pmatrix} d_{i_s} & 0 \\ 0 & d_{i_s} \end{pmatrix}$.

But all the matrices on the right are now equivalent to $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Hence $\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = 1$.

We have now proved:

Theorem 2.33

Let B be as above, $m = p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r}$. Then PSL(2,ℤ(m)) has an efficient presentation given by

$$\langle x, y \mid x^2 = (xy^4xy^{(m+1)/2})^2y^m = (xy^{-d_i})^3 = 1 \rangle$$

for each $d_i \in B$, $i = 0, 1, \ldots, r - 1$.

Example 2.34

To illustrate this theorem take $m = 3.5.7.11 = 1155$

$$E = \{\pm1, \pm34, \pm76, \pm274, \pm386, \pm419, \pm461, \pm496\}.$$

As elements of ℤ(3) x ℤ(5) x ℤ(7) x ℤ(11) they are respectively,

$\{\pm(1,1,1,1), \pm(1,-1,-1,1), \pm(1,1,-1,-1), \pm(1,-1,1,-1), \pm(-1,1,1,1)$

$\pm(-1,-1,-1,1), \pm(-1,1,-1,-1), \pm(1,1,-1,1)\}$

$B = \{(-1,-1,-1,-1), (1,-1,-1,-1), (1,1,-1,-1), (1,1,1,-1)\}$

$= \{-1, -386, 76, 736\}.$

Then the following is an efficient presentation for PSL(2,ℤ(1155))

$$\langle x, y \mid x^2 = (xy^4xy^{(m+1)/2})^2y^{1155} = (xy)^3 = (xy^{386})^3 = 1,$$

$$(xy^{-76})^3 = (xy^{419})^3 = 1 \rangle.$$

Chapter III. Presentations for the groups $SL(2,2^n)$.

J.A. Todd gave a presentation for the groups $SL(2,2^n)$ in [19]. The number of generators and relations he used increased with n. Sinkov improved upon this presentation [16] but still the number of defining relations increased with n.

In this chapter, we continue the step forward made by Sinkov and produce a presentation on three generators, requiring at most seven defining relations. We reduce this further to a deficiency -1 or -2 presentation.

Todd's original presentation uses a primitive element of $GF(2^n)$ satisfying an irreducible polynomial over GF(2). We investigate what happens when the polynomial used in this presentation is not irreducible and obtain, under suitable conditions, a presentation for a direct product groups $SL(2,2^{n_i})$ where $(n_i,n_j)= 1$.

In 1936, Todd [19] obtained a presentation for the groups $SL(2,2^n)$ using n+2 generators and $\binom{n+2}{2}+ 3$ defining relations. Apart from small values of n, this was a simpler presentation than earlier ones. In 1939, Sinkov [16] reduced Todd's presentation and showed that on generators U, R, and S, the following n+5 relations are sufficient to define $SL(2,2^n)$.

$$\left.\begin{aligned} &R^{2^n-1} = S^2 = U^3 = (UR)^2 = (US)^2 = 1 \\ &SRS^{a_1}R^{-1}R^2S^{a_2}R^{-2}\ldots R^{n-1}S^{a_{n-1}}R^{1-n}R^nSR^{-n} = 1 \\ &(SR^iSR^{-i})^2 = 1, \quad i = 1, 2, \ldots, n-1 \end{aligned}\right\} \quad (3.1)$$

where the a_i's are the coefficients of the irreducible polynomial

$$p(x) = \sum_{i=0}^{n} a_i x^i \qquad \text{over GF(2)},$$

satisfied by a primitive element α of $GF(2^n)$, $a_0 = a_n = 1$. The relations $(SR^iSR^{-i})^2 = 1$, $i = 1, 2, \ldots, n-1$, are equivalent to the relations $[S,R^iSR^{-i}] = 1$, $i = 1, 2, \ldots, n-1$, since S has order two. We prefer to use the latter. The number of defining relations increases with n because of these commutator relations. We shall try to reduce (3.1) by removing as many commutators as we can. First attempts were made using COSET. For $n = 3$, the polynomial

$$x^3 + x + 1$$

is irreducible and satisfied by a primitive element of GF(8). Using COSET it proved possible to remove all the commutators showing that SL(2,8) can be presented as,

$$\langle U, R, S \mid U^3 = (UR)^2 = (US)^2 = S^2 = R^7 = R^3SR^{-2}SR^{-1}S = 1 \rangle$$

For $n = 4$, the polynomial

$$x^4 + x + 1$$

is irreducible over GF(2) and satisfied by a primitive element of GF(16). Again, using COSET, we found that all the commutator relations could be removed. However, we found cases where some but not all commutators could be removed. Whenever the irreducible polynomial was a trinomial, we found most redundancy.

Definition 3.1

We define the groups H(m,k,j) as

$$\langle a, b \mid a^2 = b^m = 1, b^k a\, b^{-k} = a\, b^j a\, b^{-j} \rangle \qquad (3.2)$$

for m odd and $(j,m) = 1$.

The following result is joint work with C.M. Campbell, J.M. Cohen and E.F. Robertson.

Theorem 3.2

The derived group of H(m,k,j) is abelian of exponent two.

Proof (See also Campbell and Robertson, Proc. Edinburgh Math. Soc. 23 (1980))

Adding the relation [a,b] = 1 to (3.2) gives the presentation for H(m,k,j) factored by its derived group. It reduces to

$$\langle b \mid b^m = 1 \rangle ,$$

showing that the index of H'(m,k,j) in H(m,k,j) is m. We apply the modified Todd-Coxeter algorithm to H(m,k,j) using the subgroup K generated by

$$\{a,\ bab^{-1},\ b^2ab^{-2},\ \ldots,\ b^{m-1}ab^{1-m}\}.$$

Let $x_i = b^iab^{-i}$, i = 0,1,...,m-1. We set up the subgroup generator tables and relation tables as usual.

a	b	a	b^{-1}
1	1	2	2	1

b	b	a	b^{-1}	b^{-1}	....	b^{m-1}	a	b^{1-m}
1	2	3	3	2	1	1	m	m	1

a	a
i	i	i

b (m)	b	. . .	b
i	i+1		i-1	i

b (k)	b...b	a	b^{-1} (k)	b^{-1}...b^{-1}	b (j)	b...b	a	b^{-1} (j)	b^{-1} ... b^{-1}	a
i		i+k	i+k		i		i+j	i+j		i	i

From the first subgroup generator table we have

$$1\ a = x_o.1 .$$

Define the coset representatives

$$i\ b = 1.(i+1) , \quad i = 1, 2, \ldots, m-1.$$

The first row of the second relation table now completes giving

the extra information m,b = 1.1. From each of the remaining subgroup generator tables, we obtain

$$i\ a = x_{i-1}.i, \qquad i = 2,3,\ldots,m.$$

The tables now complete with no coincidence, and the coset table is:

$$\left.\begin{array}{l} i\ a = x_{i-1}.i \\ i\ b = 1.(i+1) \end{array}\right\} \quad i = 1,2,\ldots,m\ ,$$

where by coset m+1 we mean coset 1.

Hence K has index m in H(m,k,j). Since $a \in H'(m,k,j)$ and $[a,b^{-j}] \in H'(m,k,j)$, then

$$a\ a^{-1}b^{j}a\ b^{-j} = b^{j}a\ b^{-j} \in H'(m,k,j).$$

This shows that $K \leq H'(m,k,j)$. Therefore, $K = H'(m,k,j)$.

A presentation for K is now obtained, the relations coming from each row of each relation table. The relations are;

$$x_{i-1}^{2} = 1$$

$$x_{i+k-1}x_{i+j-1}x_{i-1} = 1$$

where $i = 1,2,\ldots,m$.

That is, (writing x_o as x_m)

$$\left.\begin{array}{l} x_i^2 = 1 \\ x_{i+k} = x_i\ x_{i+j} \end{array}\right\} \quad i = 1,2,\ldots,m \qquad (3.3)$$

It remains for us to show K is abelian.

$$x_{i+k}^2 = 1 \Rightarrow (x_i\ x_{i+j})^2 = 1, \quad i = 1,2,\ldots,m.$$

Therefore,

$$x_i\ x_{i+j} = x_{i+j}^{-1}\ x_i^{-1} = x_{i+j}\ x_i, \quad i = 1,2,\ldots,m\ ,$$

since every generator has order two. So, $[x_i,x_{i+j}] = 1$, $i = 1,2,\ldots,m$.

Assume that for some $r \in \mathbb{N}$

$$[x_i, x_{i+rj}] = 1 \tag{3.4}$$

and

$$x_{i+rk} = x_i \, x_{i+j}^{r,1} \, x_{i+2j}^{r,2} \cdots x_{i+(r-1)j}^{r,r-1} \, x_{i+rj} \tag{3.5}$$

where the exponent r,j denotes the binomial coefficient $\binom{r}{j}$.

$$x_{i+(r+1)k} = x_{i+rk} \, x_{i+rk+j}$$

$$= (x_i \, x_{i+j}^{r,1} \cdots x_{i+(r-1)j}^{r,r-1} \, x_{i+rj})(x_{i+j} \, x_{i+2j}^{r,1} \cdots x_{i+rj}^{r,r-1} x_{i+(r+1)j}).$$

The only terms which do not commute in this last expression are x_i and $x_{i+(r+1)j}$. Also, since

$$\binom{r}{i} + \binom{r}{i-1} = \binom{r+1}{i}$$

then

$$x_{i+(r+1)k} = x_i \, x_{i+j}^{r+1,1} x_{i+2j}^{r+1,2} \cdots x_{i+rj}^{r+1,r} \, x_{i+(r+1)j} = x_i w x_{i+(r+1)j},$$

say, showing (3.5) holds for r+1.

Also, $(x_i \, w \, x_{i+(r+1)j})^2 = 1$ which implies

$$x_i \, w \, x_{i+(r+1)j} = x_{i+(r+1)j} \, w \, x_i$$

$$x_i \, x_{i+(r+1)j} = x_{i+(r+1)j} \, x_i$$

since w commutes with x_i and $x_{i+(r+1)j}$.

Therefore (3.4) holds for r+1. (3.4),and (3.5) hold when r = 1, and so for all $r \in \mathbb{N}$. But as (j,m) = 1, the relations

$$[x_i, x_{i+rj}] = 1 \qquad i = 1,2,\ldots,m$$

show that all elements commute. Hence K is abelian.

Corollary 3.3

If $m = 2^n-1$ and the trinomial

$$x^k + x^j + 1 \qquad\qquad k < 2^n-1$$

has N roots in $GF(2^n)$, then $|H(m,k,j)| = 2^N.m$.

Proof

The relation matrix for $H'(m,k,j)$ is $\begin{pmatrix} M_1 \\ M_2 \end{pmatrix}$ where M_1 is the m x m diagonal matrix (2, 2, ..., 2) and M_2 the m x m circulant matrix whose first row has a 1 in the first, j^{th} and k^{th} positions and 0 otherwise. We can perform elementary row operations on M_2 working mod 2 since at each stage we can subtract a multiple of any row of M_1. By lemma 1.31, M_2 has rank $2^n - 1 - N$, where N is the number of non-zero roots of the trinomial. By theorem 1.23 and the discussion following that, M_2 can be reduced to a diagonal matrix $(d_1, d_2, \ldots, d_r, 0, 0, \ldots, 0)$ where $r = 2^n - 1 - N$ and each $d_i = 1$. Clearly, the relation matrix reduces to:

$$\begin{array}{c} \\ 1 \\ 1 \\ \\ \\ \\ \\ \\ \\ \\ \\ \hline \\ \end{array}\!\!\begin{array}{c} \overset{r}{} \\ \begin{pmatrix} \\ \\ \ddots \\ \\ 1 \\ 2 \\ \\ \ddots \\ \\ 2 \\ \hline \\ 0 \end{pmatrix} \end{array}$$

showing that $|H'(m,k,j)| = 2^N$ and $|H(m,k,j)| = 2^N.m$.

Corollary 3.4

The relations

$$[a, b^i a b^{-i}] = 1 \qquad i = 1,2,\ldots,k-1$$

hold in $H(m,k,j)$.

This result is the key to reducing the presentation (3.1). The following theorem, which was joint work with C. M. Campbell, J. M. Cohen and E. F. Robertson, shows how to reduce (3.1).

Theorem 3.5

Let x be a primitive element of $GF(2^n)$ satisfying the irreducible polynomial p(y) of degree n over GF(2). That is

$$p(x) = 0.$$

Suppose further, x satisfies a trinomial

$$1 + x^j = x^k$$

where $(j, 2^n - 1) = 1$. Then, $SL(2,2^n)$ can be presented as

$$\langle U, R, S \mid U^3 = (UR)^2 = (US)^2 = R^{2^n-1} = S^2 = 1,\ R^kSR^{-k} = SR^jSR^{-j}, R^nSR^{-n} = SRS^{a_1}R^{-1}.R^2S^{a_2}R^{-2}\ldots R^{n-1}S^{a_{n-1}}R^{1-n} \rangle$$

where the a_i's are the coefficients of p(x). Moreover, such a trinomial always exists.

Proof

The generators U, R, and S in (3.1) are satisfied by the matrices:

$$U \longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad R \mapsto \begin{pmatrix} x & 1 \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} x^t & x^{t-1} \\ 0 & x^{t-1} \end{pmatrix}$$

where $t = 2^{n-1}$ and $S \longmapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

Using the matrices, it is easy to check that the relation

$$R^kSR^{-k} = SR^jSR^{-j} \tag{3.6}$$

holds in (3.1). Now R and S satisfy the relations of H(m,k,j) with $m = 2^n - 1$. By corollary 3.4 the relations

$R^{2^n-1} = S^2 = 1$ and (3.6) imply the commutator relations. Therefore, the commutator relations are redundant and may be removed. The remaining relations are sufficient to define $SL(2,2^n)$.

As to the existence of such a trinomial, since x is primitive in $GF(2^n)$, then every non-zero element of $GF(2^n)$ is a power of x. In particular, $\exists k \in \mathbb{N}$ with

$$1 + x = x^k$$

and $(1, 2^n-1) = 1$.

Corollary 3.6

With the notation of theorem 3.5, if $p(x)$ is a primitive irreducible trinomial of degree n over GF(2) with

$$p(x) = 1 + x^j + x^n, \qquad (j,2^n-1) = 1,$$

then $SL(2,2^n)$ is isomorphic with

$$\langle U,R,S \mid U^3 = (UR)^2 = R^{2^n-1} = S^2 = (US)^2 = 1, \quad R^n S R^{-n} = S R^j S R^{-j} \rangle . \qquad (3.7)$$

Proof

The last two relations in theorem 3.5 are the same and one of these can be omitted.

Remarks

1. It is not known whether a primitive irreducible trinomial of degree n exists for every $n \in \mathbb{N}$.

2. Computer evidence suggests that the condition $p(x)$ must be satisfied by a primitive element of $GF(2^n)$ can be weakened to merely $p(x)$ being irreducible. For example, the trinomial $1 + x + x^9$ is irreducible over GF(2) but not primitive. However, using the presentation in corollary 3.6 with this trinomial, COSET shows this group is $SL(2,2^9)$.

In fact one can do better than theorem 3.5 suggests. The next theorem extends a result of J.M. Cohen (private communication).

Theorem 3.7

Let x be a primitive element of $GF(2^n)$ satisfying the trinomial

$$x^k = 1 + x^j , \qquad (j,2^n-1) = 1.$$

If the trinomial has precisely n roots in $GF(2^n)$, then $SL(2,2^n)$ is isomorphic with

$\langle U, R, S \mid U^3 = (UR)^2 = (US)^2 = R^{2^n-1} = S^2 = 1, R^kSR^{-k} = SR^jSR^{-j} \rangle$

Proof

Let G be the group above and $H = \langle R,S \rangle \leqslant G$. By Von Dyck's theorem and theorem 3.5, G has $SL(2,2^n)$ as a homomorphic image. By corollary 3.3,

$$|H| \leqslant 2^n(2^n-1).$$

If N is the normal subgroup of G such that $G/N \equiv SL(2,2^n)$, then

$$SRS^{a_1}R^{-1}R^2S^{a_2}R^{-2}\ldots R^{n-1}S^{a_{n-1}}R^{1-n}R^nSR^{-n} \in H \cap N.$$

If we can show $H \cap N = 1$, then we are done. HN/N is the subgroup of $SL(2,2^n)$ of upper triangular matrices generated by $\begin{pmatrix} x & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, the order of which is $2^n(2^n-1)$. Therefore, $HN/N \equiv H/(H \cap N)$ implies $H \cap N = 1$, and so G is $SL(2,2^n)$.

Example 3.8

To exhibit this theorem, consider the polynomial

$$x^5 + x^4 + x^3 + x^2 + 1$$

which is irreducible over GF(2) and satisfied by a primitive element α of GF(32). The trinomial

$$t_1(x) = 1 + x^2 + x^9 = (1+x^3+x^4)(1+x^2+x^3+x^4+x^5)$$

is such that $t_1(\alpha) = 0$ and there are precisely 5 roots in GF(32) since $1+x^3+x^4$ has no roots in GF(32). Also, (2,31) = 1. Alternatively,

$$t_2(x) = 1 + x + x^{20}$$
$$= (1+x+x^2)(1+x^2+x^3+x^4+x^5)(1+x^4+x^7+x^9+x^{10}+x^{11}+x^{13})$$

is satisfied by α, that is, $t_2(\alpha) = 0$. As the polynomials $1+x+x^2$, $1+x^4+x^7+x^9+x^{10}+x^{11}+x^{13}$ are irreducible over GF(2), and have no roots in GF(32), then $t_2(x)$ has precisely 5 roots in GF(32).

Thus the following are presentations for SL(2,32):

$$\langle U, R, S \mid U^3 = (UR)^2 = (US)^2 = R^{31} = S^2 = 1,\ R^9SR^{-9} = SR^2SR^{-2} \rangle$$

$$\langle U, R, S \mid U^3 = (UR)^2 = (US)^2 = R^{31} = S^2 = 1,\ R^{20}SR^{-20} = SRSR^{-1} \rangle.$$

To show that the relation

$$R^5S\,R^{-5} = S\,R^2S\,R^{-2}R^3S\,R^{-3}R^4S\,R^{-4}$$

does hold, then in the first of these, using the fact that

$$[R^jS\,R^{-j},\ R^kS\,R^{-k}] = 1 \qquad 1 \leq j < k \leq 30$$

it is easy to show

$$R^{40}S\,R^{-40} = R^3S\,R^{-3}R^4S\,R^{-4}R^5S\,R^{-5}.$$

Since $R^{31} = 1$, this becomes

$$R^9S\,R^{-9} = R^3S\,R^{-3}R^4S\,R^{-4}R^5S\,R^{-5}.$$

Therefore,

$$S\,R^2S\,R^{-2} = R^3S\,R^{-3}R^4S\,R^{-4}R^5S\,R^{-5}$$

as required.

We have now succeeded in showing that on three generators, at most seven relations are needed to define $SL(2,2^n)$. Apart from small values of n, this improves upon earlier presentations.

In 1899, Burnside (see [7], p97) gave a two generator, four relation presentation for SL(2,8). Sinkov (see [7], p97) gave presentations for SL(2,16) and SL(2,32) on two generators with five and six defining relations, respectively. Campbell and Robertson have found deficiency zero presentations for SL(2,8) and SL(2,16). These appear in [3] and [13], respectively. We shall now reduce our presentation.

Lemma 3.9

With the notation of theorem 3.5, $SL(2,2^n)$ is isomorphic with

$$\langle U, R, S \mid U^3 = (US)^2,\ R^{2^n-1} = S^2 = (UR)^2 = 1,\ R^k S R^{-k} = S R^j S R^{-j}$$

$$R^n S R^{-n} = S R S^{a_1} R^{-1} R^2 S^{a_2} R^{-2} \ldots R^{n-1} S^{a_{n-1}} R^{1-n} \rangle$$

Proof

$$U^3 = USUS$$

$$\Rightarrow U^2 = SUS$$

$$\Rightarrow U^{-1} S U = US.$$

Therefore $(US)^2 = U^{-1} S^2 U = i$.

Theorem 3.10

With the notation of theorem 3.5, for $n \geq 3$, $SL(2,2^n)$ has a deficiency -2 presentation which is

$$\langle U, R, S \mid U^3 = (US)^2,\ R^{2^n-1} = S^2 = (UR)^2,\ R^k S R^{-k} = S R^j S R^{-j},$$

$$R^n S R^{-n} = S R S^{a_1} R^{-1} \ldots R^{n-1} S^{a_{n-1}} R^{1-n} \rangle$$

Proof

Let G be the group above. G is perfect. Let $A = \langle S^2 \rangle$. S^2 commutes with R, S and UR, and clearly G is generated by these three elements. Therefore, $A \leq Z(G) \cap G'$. By lemma 3.9, $G/A \equiv SL(2,2^n)$ and so G is a stem extension of $SL(2,2^n)$. For $n \geq 3$, as $M(SL(2,2^n)) = 1$, by theorem 1.19, then $SL(2,2^n)$ is its own stem extension. Hence $G \equiv SL(2,2^n)$.

There are two immediate consequences of this.

Corollary 3.11

If p(x) is a primitive irreducible trinomial of degree n over GF(2),

$$p(x) = 1 + x^j + x^n \qquad (j, 2^n-1) = 1,$$

then $SL(2,2^n)$ has a deficiency -1 presentation given by

$\langle U, R, S \mid U^3 = (US)^2, R^{2^n-1} = S^2 = (UR)^2, R^n S R^{-n} = S R^j S R^{-j} \rangle$.

Proof

Using corollary 3.6, the arguments of lemma 3.9 and theorem 3.10 still hold.

Corollary 3.12

If x is primitive in $GF(2^n)$ and satisfies the trinomial

$$x^k = 1 + x^j$$

where $(j, 2^n-1) = 1$, and if the trinomial has precisely n roots in $GF(2^n)$ then $SL(2,2^n)$ has a deficiency -1 presentation given by $\langle U, R, S \mid U^3 = (US)^2, R^{2^n-1} = S^2 = (UR)^2, R^k S R^{-k} = S R^j S R^{-j} \rangle$.

Proof

Using theorem 3.7, the proofs in lemma 3.9 and theorem 3.10 still hold.

J.M. Cohen has since given an implicit deficiency -1 presentation for $SL(2,2^n)$, for all n. His proof uses the following facts.

1. Sinkov [16] shows that U and R generate $SL(2,2^n)$. Since all elements of order two are conjugate (see [8]), there is a word $w = w(U,R)$ in $SL(2,2^n)$ such that $S = w^{-1}(UR)w$.

2. $1+x^j+x^k \equiv 0 \pmod{p(x)}$. Therefore, $1+x^j+x^k = r(x)p(x)$ for some $r(x) \in GF(2)[x]$. The trinomial has no repeated factors provided j or k is odd. Therefore, r(x) and p(x) are coprime. Hence, $a(x), b(x) \in GF(2)[x]$ with

$$r(x)a(x) + p(x)b(x) = 1.$$

Let $q(x) = r(x)a(x)$. Then q(x) has the following properties.

(i) p(x) divides q(x) with a remainder of 1.

(ii) r(x) divides q(x).

The existence of $q(x)$ is necessary in Cohen's proof.

We remarked earlier that using an irreducible trinomial in (3.1) instead of a primitive trinomial, often yields a presentation for $SL(2,2^n)$. If $t(x)$ is a trinomial over GF(2) with root α,

$$1 + \alpha^j = \alpha^n$$

and $\alpha^m = 1$, with $(j,m) = 1$, what is the group defined by

$\langle U, R, S \mid U^3 = (UR)^2 = (US)^2 = R^m = 1, R^n S R^{-n} = S R^j S R^{-j} \rangle$?

More generally, what is the group defined in (3.1) when our polynomial is not irreducible or primitive? Unfortunately, we cannot say in general. Theorem 3.7 does provide some answers. Also, under suitable conditions, we know the answer. First we need to develop some ideas.

Let $F_2[x]$ denote the ring of polynomials over GF(2). Let $m(x) \in F_2[x]$ be given by

$$m(x) = p_1(x)p_2(x)\ldots p_r(x),$$

where the $p_i(x)$ are primitive irreducible polynomials of degree n_i satisfying $(n_i,n_j) = 1$, $1 \leqslant i < j \leqslant r$, and assume $n_i \geqslant 2$. Then deg $m(x) = n_1+n_2+\ldots+n_r = N$ say.

Lemma 3.13

With the above definitions,

$$F_2[x]/\langle m(x)\rangle \equiv \bigoplus_{i=1}^{r} GF(2^{n_i}).$$

Proof

$\bigoplus_{i=1}^{r} GF(2^{n_i})$ is a ring under component addition and multiplication, and has order 2^N. $F_2[x]/\langle m(x)\rangle$ also has order 2^N and can be thought of as the ring of polynomials of degree less than N with addition and multiplication done mod m(x). Define

$$\phi: \frac{F_2[x]}{m(x)} \longrightarrow \bigoplus_{i=1}^{r} GF(2^{n_i})$$

by $f \longmapsto (f_1, f_2, \ldots, f_r)$ where $f_i \equiv f \pmod{p_i(x)}$.

ϕ is injective since $(f_1, f_2, \ldots, f_r) = (g_1, g_2, \ldots, g_r)$ implies $f_i = g_i$, $i = 1,2,\ldots,r$, and so $f+g \equiv 0 \pmod{p_i}$, $i = 1,2,\ldots,r$. As each $p_i(x)$ divides f+g, then so does m(x). Hence, $f \equiv g \pmod{m(x)}$. Since we are dealing with equipotent sets, ϕ is bijective.

$$(f+g)\phi = (f_1+g_1, f_2+g_2, \ldots, f_r+g_r) = (f_1, f_2, \ldots, f_r)+(g_1, g_2, \ldots g_r)$$

$$= f\phi+g\phi.$$

If $f_i \equiv f \pmod{p_i(x)}$, then $\exists\, q_i(x) \in F_2[x]$ with

$$f = f_i + p_i(x)q_i(x).$$

Similarly, $$g = g_i + p_i(x)r_i(x).$$

Then, $$fg = f_ig_i + p_i(x).(g_iq_i + p_ir_iq_i + f_ir_i),$$

and so

$$fg \equiv f_ig_i \pmod{p_i(x)},\ i = 1,2,\ldots,r.$$

$$(fg)\phi = (f_1g_1, f_2g_2, \ldots, f_rg_r) = (f_1, f_2, \ldots, f_r)(g_1, g_2, \ldots, g_r)$$

$$= f\phi g\phi.$$

ϕ is therefore an isomorphism.

Lemma 3.14

If (n,m) = 1, then $(2^n-1, 2^m-1) = 1$, where $n,m \in \mathbb{N}$.

Proof

$\exists x, y \in \mathbb{N}$ such that $nx - my = 1$ or $my - nx = 1$. Without loss of generality, suppose $nx - my = 1$. Then, $nx = 1 + my$, and

$$2^{nx} = 2.2^{my} = 2^{my} + 2^{my},$$

whereupon

$$(2^{nx}-1) - (2^{my}-1) = 2^{my}.$$

Let $t = (2^n-1, 2^m-1)$. t divides 2^n-1, 2^m-1 and so divides $2^{nx}-1$ and $2^{my}-1$. This is because

$$2^{nx}-1 = (2^n-1)(1 + 2^2 + 2^{2n} + \ldots + 2^{n(x-1)}).$$

Therefore t divides 2^{my}. But t is odd since 2^n-1 is odd, and so we must have $t = 1$.

The following lemma is stated without proof. (The proof can be found in ' Algebraic Coding Theory' by E.R. Berlekamp, McGraw-Hill ,(1968)).

Lemma 3.15

Let $f(x) = p_1(x)p_2(x)\ldots p_r(x)$ where the $p_i(x)$ are irreducible polynomials of degree n_i over GF(2). Suppose the period of $p_i(x)$ in $GF(2^{n_i})$ is m_i. Then the least j for which $f(x)$ divides x^j-1 is the lowest common multiple of the m_i.

Let $A_m = F_2[x]/\langle m(x) \rangle$ where $m(x)$ is as above. Then the least j for which $m(x) \mid x^j-1$ in $F_2[x]$ is given by

$$j = (2^{n_1}-1)(2^{n_2}-1)\ldots(2^{n_r}-1),$$

since the $p_i(x)$ are irreducible and primitive. In A_m, $m(x) = 0$ and so we can think of x as a root of $m(x)$. It follows that on putting $m_i = 2^{n_i}-1$, and $n = m_1m_2\ldots m_r$ that $x^n \equiv 1 \pmod{m(x)}$.

By lemma 3.13, we can think of each element in A_m as an r-tuple in $\bigoplus_{i=1}^{r} GF(2^{n_i})$. In particular we have

$$0 = (0,0,\ldots,0),\ 1 = (1,1,\ldots,1) \text{ and } x = (x_1,x_2,\ldots,x_r)$$

where x_i satisfies $x_i^{m_i} = 1$ in $GF(2^{n_i})$, and so is a field generator. We note that the zero divisors in A_m correspond to an r-tuple with at least one zero. Also, there are n invertible elements in A_m, and each is of the form x^k, for some k, $1 \leqslant k \leqslant n$.

Lemma 3.16

With the notation as above, m(x) splits over the field $GF(2^v)$ where $v = n_1n_2n_3\ldots n_r$.

Proof

We can assume $n_1 < n_2 < \ldots < n_r$. Now, m(x) has no root in $GF(2) = F_2$. Adjoin a root α_1, such that $p_1(\alpha_1) = 0$. Then, $p_1(x)$ splits completely over $GF(2^{n_1}) = F_2(\alpha_1)$.

So, $m(x) = (x+\alpha_{11})(x+\alpha_{12})\ldots(x+\alpha_{1n_1})m_2(x)$

where $m_2(x)$ is a polynomial of degree $N - n_1$. $m_2(x)$ has no roots in $F_2(\alpha_1)$ otherwise this root β, would satisfy $p_j(\beta) = 0$, for some j, and $|\beta| \mid 2^{n_1}-1$. Also, $|\beta| \mid 2^{n_j}-1$ which is impossible since $(n_i,n_j) = 1$.

So m(x) does not split over $F_2(\alpha_1)$. Adjoin a root of $p_2(x)$, α_2, to form the field $F_2(\alpha_1,\alpha_2) = GF(2^{n_1n_2})$. By the above argument

$$m(x) = (x+\alpha_{11})\ldots(x+\alpha_{1n_1})(x+\alpha_{21})\ldots(x+\alpha_{2n_2})m_3(x)$$

where $m_3(x)$ is a polynomial of degree $N - n_1 - n_2$ which is irreducible over $F_2(\alpha_1,\alpha_2)$.

Continuing, we see that m(x) splits over $F_2(\alpha_1,\alpha_2,\ldots,\alpha_r)$ where each α_i is a root of $p_i(x)$. That is, m(x) splits over $GF(2^v)$.

Definition 3.17

Let $q = 2^v$, $m(x)$ be as above. We define

$$H_o = \langle a, b \mid a^2 = b^{q-1} = a^{m(x)} = 1, [a, b^i a b^{-i}] = 1, i = 1,2,\ldots,N-1 \rangle$$

where by $a^{m(x)}$ we mean

$$a\ b\ a^{e_1} b^{-1}\ b^2\ a^{e_2} b^{-2} \ldots\ b^N a\ b^{-N}$$

the e_i's being the coefficients of

$$m(x) = \sum_{i=0}^{N} e_i x^i, \quad e_o = e_N = 1.$$

We note that since $m(x)$ has no root in GF(2), then the number of occurrences of a in $a^{m(x)}$ must be odd. Bearing this in mind, we have the following result.

Theorem 3.18

$$|H_o| = (q-1)2^N.$$

H_o' is an abelian group.

Proof

A presentation for H_o/H_o' is obtained by adding the relation $[a,b] = 1$.

$H_o/H_o' = \langle a, b \mid b^{q-1} = a^2 = a^t = 1 \rangle$ where t is the number of occurrences of a in the relation $a^{m(x)} = 1$. But t is odd and so we deduce $a = 1$. Let

$$K = \langle a, b^i a b^{-i}; i = 1,2,\ldots,q-2 \rangle$$

Clearly $K \leq H_o'$. We apply the modified Todd-Coxeter algorithm to find $|H_o : K|$ and a presentation for K. The idea is the same as in the proof of theorem 3.2, except that our polynomial is more general and we have some commutator relations. However, no problem arises and we have as a set of defining relations for K:

$$x_i^2 = 1 \qquad \left.\begin{array}{l} \\ \\ \end{array}\right\} \qquad (3.8)$$

$$[x_i, x_{i+j}] = 1, \quad j = 1,2,\ldots,N-1 \quad \left.\begin{array}{l} \\ \\ \end{array}\right\} i = 1,2,\ldots,q-1 \qquad (3.9)$$

$$x_i^{e_1} x_{i+1}^{e_2} x_{i+2}^{e_3} \cdots x_{i+N-1}^{e_{N-1}} x_{i+N} = 1 \qquad \left.\begin{array}{l} \\ \\ \end{array}\right\} \qquad (3.10)$$

and $|H_o : K| = q-1$, so that $K = H_o'$.

From (3.9), we have that the elements $x_1, x_2,\ldots,x_N$ commute with one another, and so $\langle x_1, x_2,\ldots, x_N\rangle = L$, say, is abelian. (3.10) shows that x_{N+1} can be written in terms of $x_1, x_2,\ldots,x_N$ and so $x_{N+1} \in L$. Similarly, by (3.10), x_{N+2} can be written as a word in $x_2, x_3,\ldots,x_{N+1}$ and so as a word in $x_1, x_2,\ldots, x_N$. Therefore $x_{N+2} \in L$. Continuing this argument shows that x_i, $N+1 \leqslant i \leqslant q-1$, can be expressed as a word in $x_1, x_2,\ldots,x_N$. Hence $L = K$ and so K is abelian. To evaluate $|K|$ we set up the relation matrix for K and use elementary row operations to diagonalize it. By corollary 3.3 and lemma 1.31, it follows that K is the direct product of N cyclic groups of order 2, and so $|K| = 2^N$ as required. Therefore,

$$|H_o| = (q-1)\ 2^N.$$

Definition 3.19

For each $f \in A_m \setminus \{0\}$, we define

$$X_f = \{g \in A_m;\ gf + 1 = x^t,\ 1 \leqslant t \leqslant n\}$$

and

$$X_f^1 = \{x^s \in A_m;\ x^s f + 1 = x^t,\ 1 \leqslant t \leqslant n\}.$$

Lemma 3.20

Given $f \in A_m$, then every $g \in A_m$ can be written as the sum of two powers of x. Moreover, one of these is a member of X_f^1.

Proof

Let $f = (f_1, f_2, \ldots, f_s, 0, 0, \ldots, 0)$ where we can assume $f_i \neq 0$. Let $g = (g_1, g_2, \ldots, g_r)$. Choose $z = (x_1, x_2, \ldots, x_r)$ and $y = (x_1+g_1, x_2+g_2, \ldots, x_r+g_r)$ such that $x_i \neq g_i, f_i^{-1}$ or 0. y and z are both powers of x since no term in the r-tuple is zero. Clearly $y + z = g$. Also, $z \in X_f^1$ since

$$fz + 1 = (f_1x_1 + 1, f_2x_2 + 1, \ldots, f_sx_s + 1, 1, 1, \ldots, 1)$$

which is a power of x.

It is worth noting that the condition $n_i \geq 2$ is important here, as in the above proof, we have only one choice for x_i when $n_i = 2$ if g_i, f_i^{-1} and 0 are distinct elements of GF(4).

There is a strong connection between A_m and

$$H_o = \langle a, b \mid a^2 = b^{q-1} = a^{m(x)} = 1, [a, b^i a b^{-i}] = 1, i = 1,2,\ldots,N-1 \rangle$$

which we now illustrate.

$F_2[x]$ is an abelian group under addition. Define $\phi: F_2[x] \longrightarrow H_o'$ by $0\phi = 1$, $1\phi = a$, $x^j\phi = b^j a b^{-j}$, $j = 1,2,3,\ldots$, and extend by linearity. Since $[b^i a b^{-i}, b^j a b^{-j}] = 1$ in H_o, $0 \leq i < j$ and H_o' is generated by $\{a, b^i a b^{-i};\ i = 1,2,\ldots,N-1\}$, then ϕ is an epimorphism.

$$m(x)\phi = (e_o + e_1x + \ldots + e_Nx^N)\phi$$

$$= a^{e_o} b a^{e_1} b^{-1} \ldots b^N a^{e_N} b^{-N} = 1.$$

Hence $m(x) \in \text{Ker } \phi$. ϕ induces an epimorphism $\theta: A_m \longrightarrow H_o'$. If $f \in A_m$ we denote the image of f under θ as a^f. Moreover, if $f = c_o + c_1x + \ldots + c_tx^t$ (where $c_i = 0$ or 1) we have

$$(fx^j)\theta = (c_ox^j + c_1x^{j+1} + \ldots + c_tx^{t+j})\theta$$

$$= b^j a^{c_o} b^{-j} b^{j+1} a^{c_1} b^{-j-1} \ldots b^{j+t} a^{c_t} b^{-j-t}$$

$$= b^j(a^{c_0}ba^{c_1}b^{-1} \ldots b^t a^{c_t} b^{-t})b^{-j}$$

$$= b^j a^f b^{-j} = a^{fx^j}.$$

So multiplying an element of A_m by x^j corresponds to conjugating its image by b^{-j}.

We now have enough information to prove the following result. As a reminder, we have defined

$$m(x) = p_1(x)p_2(x) \ldots p_r(x)$$

where the $p_i(x)$ are irreducible primitive polynomials of degree n_i over GF(2), $n_i \geqslant 2$, satisfying $(n_i, n_j) = 1$, $1 \leqslant i < j \leqslant r$. We have set $N = n_1 + n_2 + \ldots + n_r$, $m_i = 2^{n_i} - 1$, $i = 1,2,\ldots,r$, and $n = m_1 m_2 m_3 \ldots m_r$.

Theorem 3.21

Let m(x) be a polynomial over GF(2) satisfying the above conditions. The group G =

$$\langle U, R, S \mid U^3 = (US)^2 = (UR)^2 = S^2 = R^n = S^{m(x)} = 1,\ [S, R^i S R^{-i}] = 1,\ i = 1,2,\ldots,N-1 \rangle$$

is isomorphic to

$$SL(2,2^{n_1}) \times SL(2,2^{n_2}) \times \ldots \times SL(2,2^{n_r}),$$

where by $S^{m(x)}$ we mean

$$S\ R\ S^{e_1}R^{-1}R^2S^{e_2}R^{-2}\ldots\ R^{N-1}S^{e_{N-1}}R^{1-N}R^NS\ R^{-N}.$$

Proof

The proof follows in three stages. Let H denote the subgroup generated by R and S.

(i) We shall show $|H| \leq 2^N(2^{n_1}-1)(2^{n_2}-1)\ldots(2^{n_c}-1)$. Let G_1 be the group

$$\langle R_1, S_1, U_1 \mid R_1^{q-1} = S_1^2 = (U_1R_1)^2 = U_1^3 = S_1^{m(x)} = (U_1S_1)^2 = 1,$$

$$[S_1, R_1^iS_1R_1^{-i}] = 1,\quad i = 1,2,\ldots,N-1\rangle$$

and $H_1 = \langle R_1, S_1\rangle \leq G_1$. The map $\phi: H_o \longrightarrow H_1$ defined by

$$a\phi = S_1,\ b\phi = R_1$$

extends to a homomorphism $\phi': H_o \longrightarrow H_1$ by the substitution test since $a\phi$ and $b\phi$ satisfy the relations defining H_o. Moreover, this is an epimorphism since $H_1 = \langle S_1, R_1\rangle = \langle a\phi, b\phi\rangle$. Therefore,

$$|H_1| \leq |H_o| = (q-1)2^N.$$

In G_1, $R_1^{q-1}S_1R_1^{1-q} = S_1$. But in A_m, $x^n = 1$. So, $R_1^nS_1R_1^{-n} = S_1$. Therefore R_1^n commutes with S_1.

Let $k(x) = x + x^2 + \ldots + x^{k-1}$. Then,

$$(R_1S_1)^k = R_1S_1R_1^{-1}R_1^2S_1R_1^{-2}R_1^3S_1R_1^{-3}\ \ldots\ R_1^{k-1}S_1R_1^{1-k}R_1^kS_1$$

$$= S_1^{k(x)}\ R_1^kS_1.$$

In particular,

$$(R_1S_1)^n = S_1^{n(x)}\ R_1^nS_1 = S_1^{1+n(x)}\ R_1^n = R_1^n$$

since $1 + x + x^2 + \ldots + x^{n-1} \equiv 0 \pmod{m(x)}$. This means $(R_1S_1)^n$ commutes with S_1 also.

$$(U_1R_1)^2 = 1 \Rightarrow S_1U_1R_1S_1S_1U_1R_1S_1 = 1$$

i.e.
$$(S_1U_1)R_1S_1(S_1U_1) = (R_1S_1)^{-1},$$

and as $(S_1U_1)^2 = 1$, we have

$$(S_1U_1)(R_1S_1)^n(S_1U_1) = (R_1S_1)^{-n}$$

which reduces to

$$U_1^{-1}(R_1S_1)^nU_1 = (R_1S_1)^{-n}$$

since $(R_1S_1)^n$ commutes with S_1.

But,
$$(R_1S_1)^nU_1^3 = (R_1S_1)^n$$
$$U_1(R_1S_1)^{-n}U_1^2 = (R_1S_1)^n$$
$$U_1^2(R_1S_1)^nU_1 = (R_1S_1)^n$$
$$U_1^3(R_1S_1)^{-n} = (R_1S_1)^n$$

and so

$$(R_1S_1)^{2n} = 1.$$

Hence $R_1^{2n} = 1$. Now $n \mid q-1$ since $(2^{n_i}-1) \mid (2^{n_1 n_2 \ldots n_r}-1)$, $i = 1,2,\ldots,r$. Also, $q-1$ is odd, so $R_1^{2n} = R_1^{q-1} = 1$ implies $R_1^n = 1$.

Hence $G_1 \equiv G$.

Therefore, $H = \langle R, S \rangle \leqslant G$ has order at most $2^N.n$.

That is,

$$|H| \leqslant 2^N(2^{n_1}-1)(2^{n_2}-1) \ldots (2^{n_r}-1).$$

(ii) We now show that

$$|G : H| \leqslant (2^{n_1}+1)(2^{n_2}+1) \ldots (2^{n_r}+1).$$

We have set $m_i = 2^{n_i}-1$, $i = 1,2,\ldots,r$. We shall count the cosets of H.

Clearly $H.R = H.S = H$. Define the cosets HUS^f for each $f \in A_m$, where if $f = a_o + a_1x + \ldots + a_jx^j$ then S^f means

$$S^{a_o}R\,S^{a_1}R^{-1} \ldots R^jS^{a_j}R^{-j}.$$

Clearly $HUS^fS = HUS^{f+1}$. $HUS^fR = HU^{-1}R^{-1}S^fR = HU^{-1}S^{fx^{-1}} = HUS^{1+fx^{-1}}$ and so R, S merely permute these cosets.

$$HUSU^{-1} = HU \qquad (\text{since } (US)^2 = 1)$$

$HUS^xU^{-1} = HURSR^{-1}U^{-1} = HU^{-1}SUR = HUSR = HUS^{1+x^{-1}}$.

Assume as an inductive hypothesis that $\forall\ t < s$,

$$HUS^{x^t}U^{-1} = HUS^{1+x^{-t}}.$$

Then
$$HUS^{x^s}U^{-1} = HURS^{x^{s-1}}R^{-1}U^{-1}$$
$$= HU^{-1}S^{x^{s-1}}UR$$
$$= HUS^{x^{s-1}}U^{-1}SR$$
$$= HUS^{1+x^{1-s}}SR$$
$$= HUS^{x^{1-s}}R$$
$$= HUS^{1+x^{-s}}.$$

The result holds when $t = 1$, and so holds for all values of t.

The only new cosets we get under U^{-1} are of the form

$$HUS^fU^{-1} \quad \text{where } f \neq x^s, 0 .$$

That is when f is a zero divisor. For each zero divisor f, $\forall g \in A_m$, define the cosets

$$HUS^fU^{-1}S^g.$$

Clearly, $HUS^fU^{-1}S^g.S = HUS^fU^{-1}S^{g+1}$. Also,

$$HUS^fU^{-1}S^gR = HUS^{f+1}US^{1+g}R$$
$$= HUS^{f+1}URS^{(1+g)/x}$$
$$= HUS^{f+1}R^{-1}U^{-1}S^{(1+g)/x}$$
$$= HUS^{fx}U^{-1}S^{(1+g)/x}.$$

Again, S and R merely permute these cosets.

Now, $HUS^fU^{-1}SU = HUS^{f+1}U^{-1}$. Also,

$$HUS^fU^{-1}S^xU = HUS^{f+1}US^xU^{-1}S$$
$$= HUS^{f+1}URSR^{-1}U^{-1}S$$
$$= HUS^{f+1}R^{-1}U^{-1}SURS$$
$$= HUS^{fx}U^{-1}SURS$$

$$= HUS^{fx+1}U^{-1}RS$$

$$= HUS^{(fx+1)x}U^{-1}S^{1+x^{-1}}.$$

Assume for some $t \in \mathbb{N}$,

$$HUS^{f}U^{-1}S^{x^{t}}U = HUS^{f'}U^{-1}S^{1+x^{-t}} \qquad (3.11)$$

where $f' = (fx^{t}+1)x^{t}$.

Then, $HUS^{f}U^{-1}S^{x^{t+1}}U = HUS^{f+1}US^{x^{t+1}}U^{-1}S$

$$= HUS^{f+1}URS^{x^{t}}R^{-1}U^{-1}S$$

$$= HUS^{f+1}R^{-1}U^{-1}S^{x^{t}}URS$$

$$= HUS^{fx}U^{-1}S^{x^{t}}URS$$

$$= HUS^{f'}U^{-1}S^{1+x^{-t}}RS \quad (f' = (fx^{t+1} + 1)x^{t})$$

$$= HUS^{f'x}U^{-1}S^{1+x^{-t-1}},$$

and $f'x = (fx^{t+1} + 1)x^{t+1}$, showing that (3.11) holds for t+1. (3.11) holds when $t = 1$, and so holds for all $t \in \mathbb{N}$.

In particular, suppose $x^{t} \in X_{f}^{1}$. Then,

$$HUS^{f}U^{-1}S^{x^{t}}U = HUS^{f'}U^{-1}S^{1+x^{-t}} \quad \text{by (3.11)}.$$

But $f' = (fx^{t}+ 1)x^{t}$ and so is a power of x. Therefore,

$$HUS^{f}U^{-1}S^{x^{t}}U = HUS^{1+f'^{-1}+x^{-t}+1} = HUS^{f''},$$

where $f'' = x^{-t}(fx^{t} + 1)^{-1} + x^{-t} = x^{-t}\, fx^{t}(fx^{t} + 1)^{-1} = f(fx^{t}+1)^{-1}$.

That is, $HUS^{f}U^{-1}S^{x^{t}}U = HUS^{f/(fx^{t}+1)}$.

By lemma 3.20, $\forall\, g \in A_{m}$, we have $g = x^{s} + x^{t}$ where $x^{t} \in X_{f}^{1}$. So,

$$HUS^{f}U^{-1}S^{g}U = HUS^{f}U^{-1}S^{x^{s}+x^{t}}U$$

$$= HUS^{f(1+fx^{t})^{-1}}U^{-1}S^{x^{s}}U$$

$$= HUS^{f'}U^{-1}S^{1+x^{-s}}U$$

where $f' = (\, f(1+fx^{t})^{-1}x^{s} + 1\,)x^{s}$.

Moreover, if $g \in X_f$, it follows from the above that

$$HUS^fU^{-1}S^gU = HUS^{f(1+fg)^{-1}}$$

since $fx^s(1 + fx^t)^{-1} + 1 = (fg + 1)(1 + fx^t)^{-1}$ which is a power of x. Therefore, we have shown that no new cosets arise from the list we already have.

Denote the cosets HUS^f by (f,∞) and $HUS^fU^{-1}S^g$ by (f,g). Let $B = \{(b_1, b_2, \ldots, b_r)\ ;\ b_i \in GF(2^{n_i}) \cup \{\infty\}\}$.

$|B| = (m_1+2)(m_2+2)\ldots(m_r+2)$. Define the map ψ from the list of cosets to B by

$$(f,g)\psi = (1+g_1+f_1^{-1},\ 1+g_2+f_2^{-1},\ \ldots,\ 1+g_r+f_r^{-1})$$

where $f_i = f(\text{mod } p_i(x))$ and $g_i = g(\text{mod } p_i(x))$. If $f_i = 0$, then set $f_i^{-1} = \infty$ under the rules $1/\infty = 0$, $\infty+x = \infty$.

ψ is clearly surjective. Suppose $(f,g)\psi = (f',g')\psi$. Then

$$1 + g_i + f_i^{-1} = 1 + g_i' + f_i'^{-1},\ i = 1,2,\ldots,r.$$

If $f_i = 0$, then $f_i' = 0$, and so g_i, g_i' can be anything.

For $f_i \neq 0$, $f_i' = \dfrac{f_i}{1 + f_i(g_i + g_i')}$.

Then, $f' = \dfrac{f}{1 + f(g+g')} = f(1 + f(g + g'))^{-1}$.

Now, $1 + f(g + g')$ must be a power of x since it is invertible in A_m. Therefore $g + g' \in X_f$. Hence,

$$HUS^fU^{-1}S^{g+g'}U = HUS^{f'}$$

$$\Rightarrow HUS^fU^{-1}S^g = HUS^{f'}U^{-1}S^{g'}$$

$$\Rightarrow (f,g) = (f',g').$$

If each $f_i = 0$, then $f' = f = 0$. Then,

$$HUS^fU^{-1}S^g = HUU^{-1}S^g = H = HUS^{f'}U^{-1}S^{g'}$$

and again $(f,g) = (f',g')$.

ψ is bijective, and so the the number of distinct cosets is

$$(m_1+2)(m_2+2)\ldots(m_r+2).$$

We have,

$$|G| = |H| \prod_{i=1}^{r} (m_i+2)$$

$$\leq 2^N \, n \prod_{i=1}^{r} (m_i+2)$$

$$= \prod_{i=1}^{r} 2^{n_i}(2^{n_i}-1)(2^{n_i}+1)$$

which is the order of $\underset{i=1}{\overset{r}{X}} SL(2,2^{n_i})$.

(iii) We now show that $\underset{i=1}{\overset{r}{X}} SL(2,2^{n_i})$ is a homomorphic image of G.

Define θ: $G \longrightarrow \underset{i=1}{\overset{r}{X}} SL(2,2^{n_i})$ by

$S \longmapsto (S_1, S_2, S_3, \ldots, S_r)$ where each $S_i = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

$U \longmapsto (U_1, U_2, \ldots, U_r)$ where each $U_i = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

and $R \longmapsto (R_1, R_2, \ldots, R_r)$, where

$$R_i = \begin{pmatrix} x_i^{t_i} & x_i^{t_i-1} \\ 0 & x_i^{t_i-1} \end{pmatrix} \equiv \begin{pmatrix} x_i & 1 \\ 0 & 1 \end{pmatrix}, \quad t_i = (m_i+1)/2, \; x_i \text{ being a}$$

primitive element of $GF(2^{n_i})$ satisfying $p_i(x_i) = 0$, $x_i^{m_i} \equiv 1$.

We now check that these elements do satisfy the relations of G.

$$(U_iS_i)^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

for each i, $i = 1,2,\ldots,r$. Therefore $(U\theta S\theta)^2 = 1$

$$(U_iR_i) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} x_i^{t_i} & x_i^{t_i-1} \\ 0 & x_i^{t_i-1} \end{pmatrix} = \begin{pmatrix} 0 & x_i^{t_i-1} \\ x_i^{t_i} & 0 \end{pmatrix}$$

and so $(U_iR_i)^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ since $x_i^{m_i} = 1$. This holds for each i,

so we deduce $(U\theta R\theta)^2 = 1$. Similarly, $(U\theta)^3 = (S\theta)^2 = 1$.

Now $R_i^k = \begin{pmatrix} x_i^k & \dfrac{1+x_i^k}{1+x_i} \\ 0 & 1 \end{pmatrix}$ and $R_i^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ for each i, since $m_i \mid n$.

Therefore $(R\theta)^n = 1$.

It is easy to check that

$$R_i^kS_iR_i^{-k} = \begin{pmatrix} 1 & x_i^k \\ 0 & 1 \end{pmatrix} \text{ for each i. Hence,}$$

$$S_iR_i^jS_iR_i^{-j} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & x_i^j \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1+x_i^j \\ 0 & 1 \end{pmatrix}$$

$$R_i^jS_iR_i^{-j}S_i = \begin{pmatrix} 1 & x_i^j \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1+x_i^j \\ 0 & 1 \end{pmatrix} .$$

Therefore, $[S\theta, (R\theta)^jS\theta(R\theta)^{-j}] = 1$.

If $f = a_o + a_1x + a_2x^2 + \ldots + a_sx^s \in A_m$, then

$$S_i^{f(x_i)} = S_i^{a_o}R_iS_i^{a_1}R_i^{-1}R_i^2S_i^{a_2}R_i^{-2}\ldots R_i^sS_i^{a_s}R_i^{-s}$$

$$= \begin{pmatrix} 1 & f(x_i) \\ 0 & 1 \end{pmatrix}$$

Therefore $S_i^{m(x)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ since $p_i(x_i) = 0$, and $p_i(x) \mid m(x)$, for

each i, i = 1,2,...,r.

So, by the substitution test, θ extends to a homomorphism

$$\theta' : G \longrightarrow \underset{i=1}{\overset{r}{X}} SL(2,2^{n_i}) \ .$$

Fix some i, and choose f(x) such that

$$f \equiv \begin{cases} 1 \mod p_i \\ 0 \mod p_j,\ j \neq i. \end{cases}$$

Then $S_i^f = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, while $S_j^f = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $j \neq i$.

Also, $S_i^{f+1}U_iS_i^{f+1}U_i = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, while $S_j^{f+1}U_jS_j^{f+1}U_j = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $j \neq i$.

Choose k such that $x_i^k = x_i$, $x_j^k = 1$, $j \neq i$. Then,

$$R_i^k = \begin{pmatrix} x_i & 1 \\ 0 & 1 \end{pmatrix} \text{ while } R_j^k = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad j \neq i.$$

Now by Todd's results, [19], we know that R_i^k, S_i^f, $S_i^{f+1}U_iS_i^{f+1}U_i$ generate $SL(2,2^{n_i})$. But, this holds for each i, i = 1,2,...,r. Hence Rθ, Sθ, and Uθ generate $\underset{i=1}{\overset{r}{X}} SL(2,2^{n_i})$. Therefore, θ' is an epimorphism.

Corollary 3.22

If m(x) is not a trinomial, then the root x satisfies

$$1 + x = x^k$$

for some k < n, and the presentation for $\underset{i=1}{\overset{r}{X}} SL(2,2^{n_i})$ becomes

$$\langle U, R, S \mid U^3 = R^n = (US)^2 = (UR)^2 = S^2 = S^{m(x)} = 1,\ R^kS\,R^{-k} = SRSR^{-1} \rangle$$

Proof

In A_m, 1 + x is not a zero divisor for otherwise x = 1 (mod p_i) for some i. Therefore, 1 + x is a power of x, and satisfies the above trinomial.

The relation $R^kS\,R^{-k} = S\,R\,S\,R^{-1}$ holds in the presentation in theorem 3.21 and so we may add it on. But now, by theorem 3.2 and

corollary 3.4, we may remove the commutator relations.

Corollary 3.23

If $m(x)$ is a trinomial $1 + x^j + x^N$ where $(j,n) = 1$, then the presentation in theorem 3.21 reduces to

$$\langle U, R, S \mid R^n = U^3 = (US)^2 = (UR)^2 = S^2 = 1,\ R^N S R^{-N} = S R^j S R^{-j} \rangle$$

Proof

The proof follows from theorem 3.2 and corollary 3.4.

To illustrate these results we give some examples.

Example 3.24

Let $p_1(x) = 1 + x^2 + x^3$, $p_2(x) = 1 + x + x^4$. Both are primitive, irreducible polynomials over GF(2), and satisfy $(n_1, n_2) = 1$. $m(x) = 1 + x + x^2 + x^6 + x^7$, $n = 7.15 = 105$. Also, $x^{19} = 1 + x$. By corollary 3.22, the group

$$\langle U, R, S \mid R^{105} = U^3 = (US)^2 = (UR)^2 = S^2 = 1,\ R^{19} S R^{-19} = S R S R^{-1}$$
$$R^7 S R^{-7} = S R S R S R^4 S R^{-6} \rangle$$

is $SL(2,8) \times SL(2,16)$.

Example 3.25

Take $p_1(x) = 1 + x + x^2$, $p_2(x) = 1 + x^2 + x^3$, $n = 21$, $m(x) = 1 + x + x^5$. Clearly $(1,21) = 1$. Then by corollary 3.23

$$\langle U, R, S \mid R^{21} = U^3 = (US)^2 = (UR)^2 = S^2 = 1,\ R^5 S R^{-5} = S R S R^{-1} \rangle$$

is isomorphic to $SL(2,4) \times SL(2,8)$.

We note the connection between theorem 3.7 and corollary 3.23. We saw in example 3.8 that

$$1+x+x^{20} = (1+x+x^2)(1+x+x^2+x^3+x^4+x^5)(1+x^4+x^7+x^9+x^{10}+x^{11}+x^{13}).$$

Using the polynomial $1+x+x^{20}$ in corollary 3.23 with $n = (2^2-1)(2^5-1)(2^{13}-1)$ we obtain a presentation for $SL(2,4) \times SL(2,32) \times SL(2,8192)$, since the three factors are primitive and irreducible, with $(n_i,n_j) = 1$. By theorem 3.7 we can obtain a presentation for any one of these groups by adding the relation R^3, R^{31} or $R^{8191} = 1$ to the presentation obtained from corollary 3.23.

Finally, we give some interesting examples we have found using COSET. Earlier, we asked what happens when the polynomial in (3.1) is not primitive or irreducible.

Definition 3.26

Let $m(x)$ be a polynomial of degree k over $GF(2)$, (1 not a root), and n the period of $m(x)$. We define the groups $G(n,m(x))$ to be

$$\langle U, R, S \mid U^3 = (UR)^2 = (US)^2 = S^2 = R^n = S^{m(x)} = 1, C \rangle$$

where $C = \{ [S,R^iS R^{-i}] = 1; i = 1,2,\ldots,k-1 \}$. We assume that $m(x)$ has no repeated factors.

Example 3.27

Let $m(x) = 1+x+x^2+x^3+x^4+x^5+x^6 = (1+x+x^3)(1+x^2+x^3)$. The period of $m(x)$ is 7. $G(7,m(x))$ is $SL(2,8) \times SL(2,8)$. For, if $H = \langle R,S \rangle$, using COSET we have found that $|G(7,m(x)) : H| = 567$. Also, we can deduce from the results in this chapter, that $|H| \leq 7.2^6$. The matrix pairs

$$\overline{U} = \left\{\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\right\}, \quad \overline{S} = \left\{\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right\}, \quad \overline{R} = \left\{\begin{pmatrix}x^4 & x^3\\ 0 & x^3\end{pmatrix}, \begin{pmatrix}y^4 & y^3\\ 0 & y^3\end{pmatrix}\right\}$$

satisfy the relations, where x satisfies $1+x = x^3$, and y satisfies

$1+y^2 = y^3$. Therefore there is a homomorphism from

$$G(7,m(x)) \longrightarrow SL(2,8) \times SL(2,8).$$

We note that the trinomials above are primitive and irreducible, but they need not be as the next example shows.

Example 3.28

Let $m(x) = 1+x^4+x^6+x^7+x^8 = (1+x+x^4)(1+x+x^2+x^3+x^4)$. The period of $m(x)$ is 15. $G(15,m(x))$ is $SL(2,16) \times SL(2,16)$. To show this, COSET has found $|G(15,m(x)) : \langle R, S \rangle|$ to be 4335. Again,we can show that $|\langle R,S \rangle| \leq 2^4.15$, and as above show there is a homomorphism

$$G(15,m(x)) \longrightarrow SL(2,16) \times SL(2,16).$$

The study of $G(n,m(x))$ could be quite interesting. For example, one could presumably show that the set of commutators C, can be removed whenever $m(x)$ is a trinomial of a certain type. An interesting example of this occurs for the trinomials

$$m(2^k,x) = 1 + x + x^{2^{2^k}}, \quad k \geq 2.$$

In [21] it is stated that the degree of every factor of $m(2^k,x)$ is 2^{k+1} and so there are 2^{2^k-k-1} factors. This poses the question; ' Is the group

$$\langle U, R, S \mid U^3 = (UR)^2 = (US)^2 = S^2 = R^n = 1, \; R^{2^{2^k}} SR^{-2^{2^k}} = SRSR^{-1} \rangle$$

isomorphic to 2^{2^k-k-1} copies of $SL(2,2^{2^{k+1}})$, where n is the period of $m(2^k,x)$? '

Unfortunately, even the smallest case $k = 2$,

$$m(4,x) = 1+x+x^{16} = (1+x+x^3+x^4+x^5+x^6+x^8)(1+x^3+x^5+x^6+x^8)$$

is beyond our computer resources.

Chapter IV. Presentations for PSL(2,p^n), p an odd prime.

In this chapter, we shall look at the presentations for PSL(2,p^n) given by Todd in [19], where p is an odd prime. In particular, we aim to reduce Todd's presentation so that the number of defining relations does not increase with n. Sinkov [16] has done some of the work for us, but still the number of defining relations increases with n. Sinkov points out that even the four generators he uses {U, R, S_o, S_1} are not all independent since U and R will generate the group except when $p^n = 9$.

By analogy with the case of SL(2,2^n), we are able to show that at most thirteen relations are needed to define PSL(2,p^n), using the above four generators. When $p^n \equiv -1 \pmod 4$, there is far more redundancy in the relations, and one of the above generators is eliminated.

Throughout this chapter, we shall assume p is an odd prime.

As well as giving a presentation for SL(2,2^n), Todd [19] also gives a presentation for the groups PSL(2,p^n), where p is an odd prime, on n+2 generators and $\binom{n+2}{2} + 3$ relations. He requires one extra relation if $p^n \equiv 1 \pmod 4$.

Sinkov [16] showed that Todd's presentation can be reduced. Sinkov showed that on the generators U, R, S_o, and S_1 the relations

$$U^3 = (UR)^2 = (US_o)^2 = R^m = S_o^p = S_1^p = 1 \tag{4.1}$$

$$S_o S_i = S_i S_o \qquad i = 1,2,\ldots,n-1 \tag{4.2}$$

$$S_1 S_j = S_j S_1 \qquad j = 2,3,\ldots,n-1 \tag{4.3}$$

$$RS_{n-2} = S_o^{a_o} S_1^{a_1} \ldots S_{n-1}^{a_{n-1}} R \tag{4.4}$$

$$RS_{n-1} = S_o^{b_o} S_1^{b_1} \ldots S_{n-1}^{b_{n-1}} R \tag{4.5}$$

together with $(S_1 RU)^3 = 1$ (4.6)

if $p^n \equiv 1 \pmod 4$, are sufficient to define $PSL(2,p^n)$, where $m = (p^n-1)/2$, $S_{2i} = R^i S_o R^{-i}$ and $S_{2i+1} = R^i S_1 R^{-i}$. The a_i's are the coefficients of the polynomial

$$p(x) = x^n - \sum_{i=o}^{n-1} a_i x^i$$

which is irreducible over GF(p) and satisfied by a primitive element of $GF(p^n)$. The b_i's are defined by

$$b_o = a_{n-1} a_o$$

and $$b_i = a_{n-1} a_i + a_{i-1}, \quad i = 1,2,\ldots,n-1.$$

We shall associate the indeterminate x with the root α and think of x as being a primitive element of $GF(p^n)$.

Matrices which correspond to the generators are

$$U \longleftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \quad R \longleftrightarrow \begin{pmatrix} x & x^{-1} \\ 0 & x^{-1} \end{pmatrix}, \quad S_o \longleftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S_1 \longleftrightarrow \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

Sinkov's presentation has deficiency -2n-1 or -2n-2. It would be desirable to have a presentation whose deficiency does not decrease with n. As with the case of $SL(2,2^n)$, the deficiency of Sinkov's presentation decreases with n because of the commutator relations (4.2) and (4.3). We look at what happens when the polynomial p(x) is a trinomial. First of all, we tidy up some of the relations. (4.4) and (4.5) can be rewritten as

$$S_n = S_o^{a_o} S_1^{a_1} \ldots S_{n-1}^{a_{n-1}} \tag{4.7}$$

and $$S_{n+1} = S_o^{b_o} S_1^{b_1} \ldots S_{n-1}^{b_{n-1}} .$$

Since the S_i's commute,

$$S_{n+1} = S_o^{a_o a_{n-1}} S_1^{a_1 a_{n-1}} \dots S_{n-1}^{a_{n-1} a_{n-1}} S_1^{a_o} S_2^{a_1} \dots S_{n-1}^{a_{n-2}}$$

i.e., $S_{n+1} = (S_o^{a_o} S_1^{a_1} \dots S_{n-1}^{a_{n-1}})^{a_{n-1}} S_1^{a_o} S_2^{a_1} \dots S_{n-1}^{a_{n-2}}$

i.e. $S_{n+1} = S_1^{a_o} S_2^{a_1} \dots S_{n-1}^{a_{n-2}} S_n^{a_{n-1}}$ (4.8)

The defining relations for $PSL(2,p^n)$ are (4.1),(4.2),(4.3),(4.7), (4.8) together with (4.6) if $p^n \equiv 1 \pmod 4$. Let P denote this presentation for $PSL(2,p^n)$.

Lemma 4.1.

If $y^k - \sum_{i=0}^{k-1} c_i y^i$ is any polynomial over GF(p) satisfied by the primitive element x of $GF(p^n)$, then the relation

$$S_k = S_o^{c_o} S_1^{c_1} \dots S_{k-1}^{c_{k-1}}$$

holds in P.

Proof

Since S_i corresponds to $\begin{pmatrix} 1 & x^i \\ 0 & 1 \end{pmatrix}$ we have

$$S_o^{c_o} S_1^{c_1} \dots S_{k-1}^{c_{k-1}} = \begin{pmatrix} 1 & c_o \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & c_1 x \\ 0 & 1 \end{pmatrix} \dots \begin{pmatrix} 1 & c_{k-1} x^{k-1} \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & c_o + c_1 x + \dots + c_{k-1} x^{k-1} \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & x^k \\ 0 & 1 \end{pmatrix} = S_k.$$

Definition 4.2

We define the groups $G_p(n,m,r)$ to be

$$\langle a,b,c \mid a^n = b^p = c^p = [b,a^r c a^{-r}] = [c,a^{r+1} b a^{-1-r}] = 1$$
$$a^m b a^{-m} = b^d a^r c^e a^{-r},\ a^m c a^{-m} = c^d a^{r+1} b^e a^{-1-r} \rangle$$

where $(2r+1,n) = 1$, $d,e \not\equiv 0 \pmod p$. Let $i = 2r+1$. With this definition, we have a result analogous to that in chapter three.

Theorem 4.3

For $(d-1)^2 \not\equiv e^2 \pmod p$, the derived group of $G_p(n,m,r)$ is abelian, $n \geq 3$.

Proof

Let $G = G_p(n,m,r)$. A presentation for G/G' is (omitting commutators)

$$\langle a, b, c \mid a^n = b^{d-1}c^e = c^{d-1}b^e = c^p = b^p = 1 \rangle .$$

Now, $c^e = b^{1-d}$. If k satisfies $ek \equiv 1 \pmod p$, then $c = b^{(1-d)k}$.

So,
$$b^{(1-d)(d-1)k} = b^{-e}$$
$$b^e = b^{(d-1)^2 k}$$
$$b^{e^2} = b^{(d-1)^2}.$$

Since $e^2 \not\equiv (d-1)^2 \pmod p$, then using $b^p = 1$, we deduce $b = 1$. Similarly, $c = 1$, and so G/G' is cyclic of order n and generated by a.

Let $K = \langle b, c, a^j b\, a^{-j}, a^j c\, a^{-j}, j = 1,2,\ldots,n-1 \rangle \leqslant G$. We shall obtain a presentation for K using the modified Todd-Coxeter algorithm. First of all, we note that as $b,c \in G' \leqslant G$, then $K \leqslant G'$. We set up the subgroup generator tables and relation tables as usual. The subgroup generator tables are:

b
1 | 1

a	b	a^{-1}
1 | 2	2	1

a	a	b	a^{-1}	a^{-1}
1 | 2	3	3	2	1

...

a^{n-1}	b	a^{1-n}
1 | n	n	1

c
1 | 1

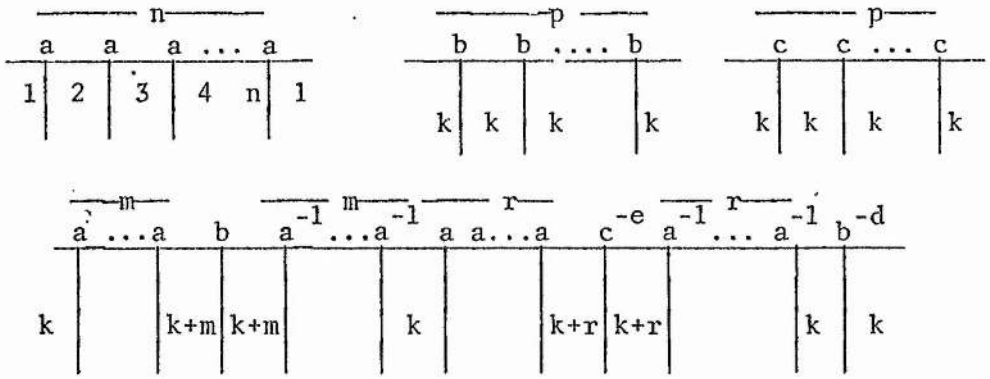
a	c	a^{-1}
1 | 2	2	1

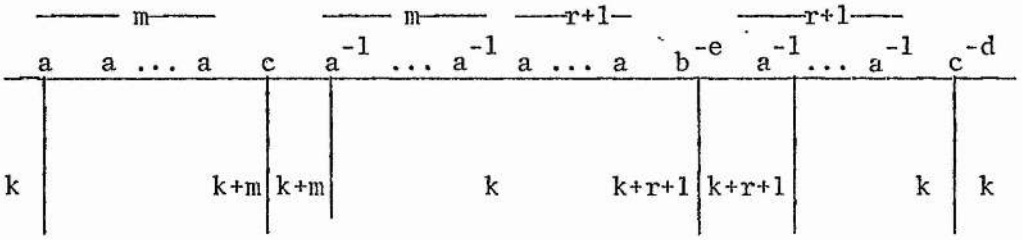
a	a	c	a^{-1}	a^{-1}
1 | 2	3	3	2	1

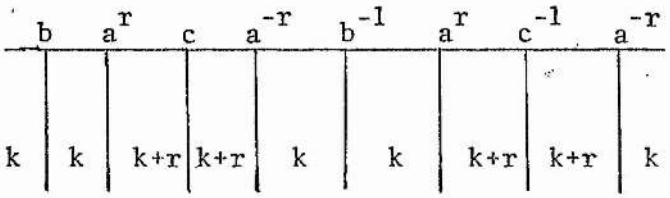
. . . .

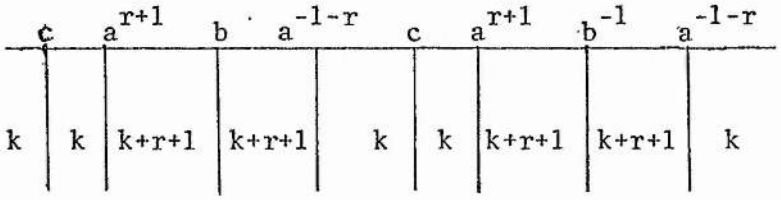
a^{n-1}	c	a^{1-n}
1 | n	n	1

and the relation tables are:









Let $b = y_1$, $c = z_1$ and $a^j b\, a^{-j} = y_{j+1}$, $a^j c\, a^{-j} = z_{j+1}$, $j = 1,2,..n-1$.

Define the coset representatives

$$k.a = 1.(k+1), \qquad k = 1,2,\ldots,n-1.$$

The first row of the first relation table now completes, giving the extra information

$$n.a = 1.1.$$

Each of the subgroup generator tables completes giving the following new information.

$$1.b = y_1.1 \qquad 1.c = z_1.1$$

$$2.b = y_2.2 \qquad 2.c = z_2.2$$

$$3\ b = y_3.3 \qquad 3.c = z_3.3$$

$$\vdots \qquad\qquad \vdots$$

and in general

$$\left.\begin{aligned} k.b &= y_k.k \\ k.c &= z_k.k \end{aligned}\right\} \qquad k = 1, 2, \ldots, n.$$

; No coincidence occurs and the tables now complete. Hence the index of K in G is n, and so K = G'. We now obtain a set of defining relations for K in terms of the generators y_k, z_k, k = 1,2,...,n . The defining relations are obtained from each row of each relation table. They are;

$$y_k^p = z_k^p = 1$$

$$y_{k+m} = y_k^d\ z_{k+r}^e$$

$$z_{k+m} = z_k^d\ y_{k+r+1}^e$$

$$[y_k, z_{k+r}] = [z_k, y_{k+r+1}] = 1 \qquad (4.9)$$

where k = 1,2,...,n.

Recall we have set i = 2r+1. Now,

$$y_{k+2m} = y_{k+m}^d\ z_{k+r+m}^e$$

$$= (y_k^d\ z_{k+r}^e)^d (z_{k+r}^d\ y_{k+2r+1}^e)^e$$

$$= y_k^{d^2} z_{k+r}^{ed}\ z_{k+r}^{ed}\ y_{k+i}^{e^2} \qquad \text{(using (4.9))} \qquad (4.10)$$

$$= y_k^{d^2} z_{k+r}^{2ed} y_{k+i}^{e^2}.$$

By lemma 1.29, since $[y_{k+m}^d, z_{k+r+m}^e] = 1$ and the only terms in (4.10) which do not commute are y_k and y_{k+i}, we deduce

$$[y_k^{d^2}, y_{k+i}^{e^2}] = 1.$$

Since $(d^2,p) = (e^2,p) = 1$, we deduce that $[y_k, y_{k+i}] = 1$, $k = 1,\ldots,n$, using lemma 1.28.

$$\begin{aligned} z_{2m+k} &= z_{m+k}^d y_{m+k+r+1}^e \\ &= (z_k^d y_{k+r+1}^e)^d (y_{k+r+1}^d z_{k+i}^e)^e \\ &= z_k^{d^2} y_{k+r+1}^{ed} y_{k+r+1}^{ed} z_{k+i}^{e^2} \end{aligned} \tag{4.11}$$

using (4.9). Again, using lemma 1.29, since

$$[z_{m+k}^d, y_{m+k+r+1}^e] = 1$$

and the only terms in (4.11) which do not commute are z_k and z_{k+i}, we deduce

$$[z_k^{d^2}, z_{k+i}^{e^2}] = 1.$$

By lemma 1.28, we deduce

$$[z_k, z_{k+i}] = 1, \qquad k = 1,2,\ldots,n.$$

$$\begin{aligned} y_{3m+k} &= y_{k+2m}^d z_{k+r+2m}^e \\ &= (y_k^{d^2} z_{k+r}^{2ed} y_{k+i}^{e^2})^d (z_{k+r}^{d^2} y_{k+i}^{2ed} z_{k+i+r}^{e^2})^e \end{aligned}$$

using (4.10) and (4.11). Since the terms in each bracket commute, we have

$$\begin{aligned} y_{3m+k} &= y_k^{d^3} z_{k+r}^{2ed^2} y_{k+i}^{e^2 d} z_{k+r}^{ed^2} y_{k+i}^{2e^2 d} z_{k+r+i}^{e^3} \\ &= y_k^{d^3} z_{k+r}^{3ed^2} y_{k+i}^{3e^2 d} z_{k+r+i}^{e^3}. \end{aligned} \tag{4.12}$$

As above, since the only terms in (4.12) which do not commute are

y_k and z_{k+r+i}, we deduce from lemmas 1.28 and 1.29 that

$$[y_k,\ z_{k+r+i}] = 1, \quad k = 1,2,\ldots,n.$$

Similarly,

$$\begin{aligned} z_{3m+k} &= z_{2m+k}^{d}\ y_{2m+k+r+1}^{e} \\ &= (z_k^{d^2}\ y_{k+r+1}^{2ed}\ z_{k+i}^{e^2})^{d} (y_{k+r+1}^{d^2}\ z_{k+i}^{2ed}\ y_{k+r+i+1}^{e^2})^{e} \end{aligned}$$

using (4.10) and (4.11). Since the terms in each bracket commute this becomes,

$$\begin{aligned} z_{3m+k} &= z_k^{d^3}\ y_{k+r+1}^{2ed^2}\ z_{k+i}^{de^2}\ y_{k+r+1}^{ed^2}\ z_{k+i}^{2de^2}\ y_{k+r+i+1}^{e^3} \qquad (4.13) \\ &= z_k^{d^3}\ y_{k+r+1}^{3ed^2}\ z_{k+i}^{3de^2}\ y_{k+r+i+1}^{e^3}. \end{aligned}$$

But $[z_{2m+k}^{d},\ y_{2m+k+r+1}^{e}] = 1$, and $(d^3,p) = (e^3,p) = 1$. Also the only terms which do not commute in (4.13) are z_k and $y_{k+r+i+1}$, by lemmas 1.28 and 1.29, we have $[z_k,\ y_{k+r+i+1}] = 1$, $k = 1,2,\ldots,n$.

Assume $\forall\ s < t$, $s,t \in \mathbb{N}$, the following hold for any k, $k = 1,2,\ldots,n$.

$$[y_k,y_{k+si}] = [z_k,z_{k+si}] = [y_k,z_{k+r+si}] = [z_k,y_{k+r+1+si}] = 1 \qquad (4.14)$$

and

$$y_{k+2sm} = \prod_{j=0}^{s-1} y_{k+ji}^{(j,2s)}\ z_{k+r+ji}^{(j:2s)}\ y_{k+is}^{e^{2s}} \qquad (4.15)$$

$$z_{k+2sm} = \prod_{j=0}^{s-1} z_{k+ji}^{(j,2s)}\ y_{k+r+1+ji}^{(j:2s)}\ z_{k+is}^{e^{2s}} \qquad (4.16)$$

$$y_{k+(2s+1)m} = \prod_{j=0}^{s} y_{k+ji}^{(j,2s+1)}\ z_{k+r+ji}^{(j:2s+1)} \qquad (4.17)$$

$$z_{k+(2s+1)m} = \prod_{j=0}^{s} z_{k+ji}^{(j,2s+1)}\ y_{k+r+1+ji}^{(j:2s+1)} \qquad (4.18)$$

where the notation

$x^{(j,r)}$ means the exponent of x is $\binom{r}{2j} d^{r-2j} e^{2j}$, and $x^{(j:r)}$ means the exponent of x is $\binom{r}{2j+1} d^{r-2j-1} e^{2j+1}$.

Then,

$$y_{k+2tm} = y_{k+(2t-1)m}^{d} z_{k+r+(2t-1)m}^{e}$$

$$= \Big(\prod_{j=0}^{t-1} y_{k+ji}^{(j,2t-1)} z_{k+r+ji}^{(j:2t-1)}\Big)^{d} \Big(\prod_{j=0}^{t-1} z_{k+r+ji}^{(j,2t-1)} y_{k+2r+1+ji}^{(j:2t-1)}\Big)^{e}.$$

The terms within each bracket commute giving

$$y_{k+2tm} = \prod_{j=0}^{t-1} y_{k+ji}^{(j,2t-1)d} z_{k+r+ji}^{(j:2t-1)d} \prod_{j=0}^{t-1} z_{k+r+ji}^{(j,2t-1)e} y_{k+(j+1)i}^{(j:2t-1)e} \quad (4.19)$$

Now, $[y_{k+(2t-1)m}^{d}, z_{k+r+(2t-1)m}^{e}] = 1$. The only terms in (4.19) which do not commute are y_k and y_{k+ti}, by assumption. By lemma 1.29, we have

$$[y_k^{(0,2t-1)d}, y_{k+ti}^{(t-1:2t-1)e}] = 1.$$

Now $(0,2t-1)d = d^{2t-1}d = d^{2t}$. $(t-1:2t-1)e = d^{2t-1-2t+1}e^{2t-1}e = e^{2t}$.

Since $(d^{2t},p) = (e^{2t},p) = 1$, by lemma 1.28 we obtain

$$[y_k, y_{k+ti}] = 1, \quad k = 1,2,\ldots,n .$$

Moreover, (4.19) becomes (since all terms now commute)

$$y_{k+2tm} = \prod_{j=0}^{t-1} y_{k+ij}^{(j,2t-1)d} \prod_{j=0}^{t-2} y_{k+(j+1)i}^{(j:2t-1)e} \prod_{j=0}^{t-1} z_{k+r+ji}^{(j:2t-1)d + (j,2t-1)e} \cdot y_{k+ti}^{e^{2t}}$$

$$= \prod_{j=0}^{t-1} y_{k+ij}^{(j,2t-1)d + (j-1:2t-1)e} z_{k+r+ji}^{(j,2t-1)e + (j:2t-1)d} \cdot y_{k+ti}^{e^{2t}}$$

where we have taken $(-1:2t-1)e = 0$.

Now $(j,2t-1)d + (j-1:2t-1)e =$

$$\binom{2t-1}{2j} d^{2t-1-2j+1} e^{2j} + \binom{2t-1}{2j-1} d^{2t-1-2j+1} e^{2j}$$

$$= \binom{2t}{2j} d^{2t-2j} e^{2j} = (j,2t).$$

$(j:2t-1)d + (j,2t-1)e =$

$$\binom{2t-1}{2j+1} d^{2t-1-2j} e^{2j+1} + \binom{2t-1}{2j} d^{2t-1-2j} e^{2j+1}$$

$$= \binom{2t}{2j+1} d^{2t-1-2j} e^{2j+1} = (j:2t)$$

Hence,

$$y_{k+2tm} = \prod_{j=0}^{t-1} y_{k+ij}^{(j,2t)} z_{k+r+ij}^{(j:2t)} y_{k+ti}^{e^{2t}}, \quad k = 1,2,\ldots,n,$$

showing that (4.15) holds when s = t.

$$z_{k+2tm} = z_{k+(2t-1)m}^{d} y_{k+r+1+(2t-1)m}^{e}$$

$$= \Big(\prod_{j=0}^{t-1} z_{k+ji}^{(j,2t-1)} y_{k+r+1+ij}^{(j:2t-1)}\Big)^{d} \Big(\prod_{j=0}^{t-1} y_{k+r+1+ji}^{(j,2t-1)} z_{k+(j+1)i}^{(j:2t-1)}\Big)^{e}.$$

Since the terms within each bracket commute, this becomes:

$$\prod_{j=0}^{t-1} z_{k+ji}^{(j,2t-1)d} y_{k+r+1+ij}^{(j:2t-1)d} \prod_{j=0}^{t-1} y_{k+r+1+ji}^{(j,2t-1)e} z_{k+(j+1)i}^{(j:2t-1)e}. \tag{4.20}$$

As before, since the only terms in (4.20) which do not commute are z_k and z_{k+ti}, and as $[z_{k+(2t-1)m}^{d}, y_{k+r+1+(2t-1)m}^{e}] = 1$, then by lemmas 1.28 and 1.29, we deduce

$$[z_k, z_{k+ti}] = 1.$$

Also,

$$z_{k+2tm} = \prod_{j=0}^{t-1} z_{k+ji}^{(j,2t-1)d + (j-1:2t-1)e} y_{k+r+1+ij}^{(j,2t-1)e + (j:2t-1)d} \cdot z_{k+ti}^{(t-1:2t-1)e}$$

$$= \prod_{j=0}^{t-1} z_{k+ji}^{(j,2t)} \; y_{k+r+1+ij}^{(j:2t)} \; z_{k+ti}^{e^{2t}}$$

showing that (4.16) holds when s = t.

$$y_{k+(2t+1)m} = y_{k+2tm}^{d} \; z_{k+r+2tm}^{e}$$

$$= \left(\prod_{j=0}^{t-1} y_{k+ji}^{(j,2t)} \; z_{k+r+ji}^{(j:2t)} \; y_{k+it}^{e^{2t}}\right)^{d} \left(\prod_{j=0}^{t-1} z_{k+r+ij}^{(j,2t)} \; y_{k+(j+1)i}^{(j:2t)} \; z_{k+it+r}^{e^{2t}}\right)^{e}$$

$$= \prod_{j=0}^{t-1} y_{k+ji}^{(j,2t)d} \; z_{k+r+ji}^{(j:2t)d} \; y_{k+it}^{e^{2t}d} \prod_{j=0}^{t-1} z_{k+r+ij}^{(j,2t)e} \; y_{k+(j+1)i}^{(j:2t)e} \; z_{k+it+r}^{e^{2t+1}} \quad (4.21)$$

since the terms within each bracket commute. The only terms in (4.21) which do not commute are y_k and z_{k+it+r}. Since

$$[y_{k+2tm}^{d}, \; z_{k+r+2tm}^{e}] = 1,$$

then by lemma 1.29, we have

$$[y_{k+ji}^{d^{2t+1}}, \; z_{k+it+r}^{e^{2t+1}}] = 1,$$

which reduces to

$$[y_{k+ji}, \; z_{k+it+r}] = 1$$

using lemma 1.28 and $(d^{2t+1},p) = (e^{2t+1},p) = 1$.

Further,

$$y_{k+(2t+1)m} = \prod_{j=0}^{t-1} y_{k+ji}^{(j,2t)d + (j-1:2t)e} \; z_{k+r+ji}^{(j:2t)d + (j,2t)e} \; y_{k+it}^{e^{2t}d} \cdot y_{k+ti}^{(t-1:2t)e} \; z_{k+r+it}^{e^{2t+1}}$$

$$= \prod_{j=0}^{t-1} y_{k+ji}^{(j,2t+1)} \; z_{k+r+ji}^{(j:2t+1)} \; y_{k+it}^{e^{2t}d + (t-1:2t)e} \; z_{k+r+it}^{e^{2t+1}}$$

Now, $e^{2t}d + (t-1:2t)e = e^{2t}d + \binom{2t}{2t-1} de^{2t} = (2t+1)e^{2t}d = (t,2t+1)$.

$$e^{2t+1} = \binom{2t+1}{2t+1} e^{2t+1} = (t:2t+1).$$

Hence $y_{k+(2t+1)m} = \prod_{j=0}^{t} y_{k+ji}^{(j,2t+1)} \; z_{k+r+ji}^{(j:2t+1)}$ which shows (4.17)

holds when s = t.

Finally,

$$z_{k+(2t+1)m} = z_{k+2tm}^{d}\, y_{k+2tm+r+1}^{e}$$

$$= \Big(\prod_{j=0}^{t-1} z_{k+ij}^{(j,2t)}\, y_{k+r+1+ij}^{(j:2t)}\, z_{k+it}^{e^{2t}}\Big)^{d} \Big(\prod_{j=0}^{t-1} y_{k+ji+r+1}^{(j,2t)}\, z_{k+(j+1)i}^{(j:2t)}\, y_{k+it+r+1}^{e^{2t}}\Big)^{e}$$

$$= \prod_{j=0}^{t-1} z_{k+ij}^{(j,2t)d}\, y_{k+r+1+ij}^{(j:2t)d}\, z_{k+it}^{e^{2t}d} \prod_{j=0}^{t-1} y_{k+ji+r+1}^{(j,2t)e}\, z_{k+(j+1)i}^{(j:2t)e}\, y_{k+it+r+1}^{e^{2t+1}} \tag{4.22}$$

since the terms within each bracket commute.

Now, $[z_{k+2tm}^{d},\ y_{k+2tm+r+1}^{e}] = 1$. Also, the only terms in (4.22) which do not commute are z_k and $y_{k+it+r+1}$. So by lemmas 1.28 and 1.29, we deduce as before

$$[z_k,\ y_{k+it+r+1}] = 1, \quad k = 1,2,\ldots,n.$$

$$z_{k+(2t+1)m} = \prod_{j=0}^{t-1} z_{k+ij}^{(j,2t)d+(j-1:2t)e}\, y_{k+r+1+ij}^{(j:2t)d+(j,2t)e}\, z_{k+it}^{e^{2t}d} \cdot z_{k+it}^{(t-1:2t)e}\, y_{k+it+r+1}^{e^{2t+1}}$$

$$= \prod_{j=0}^{t} z_{k+ij}^{(j,2t+1)}\, y_{k+r+1+ij}^{(j:2t+1)}$$

since $e^{2t}d + (t-1:2t)e = e^{2t}d + \begin{pmatrix}2t\\2t-1\end{pmatrix}de^{2t} = \begin{pmatrix}2t+1\\2t\end{pmatrix}de^{2t} = (t,2t+1)$.

Therefore, (4.18) holds with s = t. (4.14)$\longrightarrow$ (4.18) hold for s = 1 and we have shown they hold for s = t. Hence they hold for all $s \in \mathbb{N}$

As i = 2r+1 is coprime to n, then (4.14) shows that all elements of K commute. Hence K is abelian.

We also need to consider the group defined by:

Definition 4.4

We define the groups $H_p(n,m,r)$ to be

$$\langle a, b, c \mid a^n = b^p = c^p = [b, a^r c a^{-r}] = [c, a^{r+1} b a^{-1-r}] = 1,$$

$$a^m c a^{-m} = b^d a^r c^e a^{-r},\ a^{m+1} b a^{-1-m} = c^d a^{r+1} b^d a^{-1-r} \rangle$$

where $(2r+1, n) = 1$, $d, e \not\equiv 0 \pmod{p}$. Let $i = 2r+1$.

As with $G_p(n,m,r)$, we have a similar result for $H_p(n,m,r)$.

Theorem 4.5

For $(1-e)^2 \not\equiv d^2 \pmod{p}$, the derived group of $H_p(n,m,r)$ is abelian.

Proof

The proof is very similar to that of theorem 4.3 and we shall just outline the proof. First of all, using the condition $(1-e)^2 \not\equiv d^2 \pmod{p}$, we deduce $H/H' = \langle a \mid a^n = 1 \rangle$ where $H = H_p(n,m,r)$. Again we consider the subgroup K generated by the elements b, c, $a^i b a^{-i}$, $a^i c a^{-i}$, $i = 1,2,\ldots,n-1$, and obtain a presentation for K using the modified Todd-Coxeter algorithm. The index of K in H is n and as $K \leqslant H'$, we have $K = H'$.

Letting $y_1 = b$, $y_{k+1} = a^k b a^{-k}$, $z_1 = c$, $z_{k+1} = a^k c a^{-k}$, for $k = 1,2,\ldots,n-1$, defining relations for K are found to be:

$$y_k^p = z_k^p = [y_k, z_{k+r}] = [z_k, y_{k+r+1}] = 1$$

$$z_{m+k} = y_k^d z_{k+r}^e,\ y_{m+k+1} = z_k^d y_{k+r+1}^e$$

where $k = 1,2,\ldots,n$. The proof that K is abelian is similar to that in theorem 4.3, the inductive proof based on the assumption that $\forall\ s < t$, $s,t \in \mathbb{N}$, we have the following relations:

$$z_{k+2sm} = \prod_{j=0}^{s-1} z_{k-s+ji}^{(j,2s)}\ y_{k-s+r+1+ji}^{(j:2s)}\ z_{k+2sr}^{e^{2s}}$$

$$y_{k+2sm+i} = \prod_{j=0}^{s-1} y_{k-s+1+ji}^{(j,2s)}\ z_{k+r+1-s+ij}^{(j:2s)}\ y_{k+1+2rs}^{e^{2s}}$$

$$z_{k+(2s+1)m} = \prod_{j=0}^{s} y_{k-s+ji}^{(j,2s+1)} \; z_{k+r-s+ij}^{(j:2s+1)}$$

$$y_{k+(2s+1)m+i} = \prod_{j=0}^{s} z_{k-s+ij}^{(j,2s+1)} \; y_{k+r+1-s+ij}^{(j:2s+1)}$$

$$[z_k, z_{k+si}] = [y_k, y_{k+si}] = [y_k, z_{k+r+si}] = [z_k, y_{k+1+r+si}] = 1,$$

where the exponent notation is the same as that used in theorem 4.3 .

The groups $G_p(n,m,r)$ and $H_p(n,m,r)$ can both be expressed as

$$K_p(n,k,i) = \langle a, b_o, b_1 \mid a^n = b_o^p = b_1^p = [b_o, b_i] = [b_1, b_{i+1}] = 1,$$

$$b_k = b_o^d b_i^e, \; b_{k+1} = b_1^d b_{i+1}^e \rangle$$

where $b_{2j} = a^j b_o a^{-j}$, $b_{2j+1} = a^j b_1 a^{-j}$ and i is an odd integer satisfying $(i,n) = 1$.

Clearly, if k is even, $k = 2m$, then setting $(i-1)/2 = r$ we see $K_p(n,k,i) \equiv G_p(n,m,r)$. If k is odd, $k = 2m+1$, then with $i = 2r+1$, $K_p(n,k,i) \equiv H_p(n,m,r)$.

It follows from theorems 4.3 and 4.5 that the derived group of $K_p(n,k,i)$ is abelian. With these results, we are now ready to reduce Sinkov's presentation for $PSL(2,p^n)$.

Theorem 4.6

Let x be a primitive element of $GF(p^n)$, p odd, satisfying the irreducible polynomial

$$x^n = \sum_{i=0}^{n-1} a_i x^i .$$

Suppose further that x satisfies a trinomial $x^k = d + ex^i$ where i is an odd integer coprime to $(p^n-1)/2$, and for k even $e^2 \neq (d-1)^2$

(mod p), while for k odd, $d^2 \neq (e-1)^2 \pmod{p}$. Then the group generated by U, R, S_o, S_1 subject to the relations

$$\left.\begin{aligned} &U^3 = (UR)^2 = (US_o)^2 = 1 \\ &\text{with } (S_1RU)^3 = 1 \text{ if } p^n \equiv 1 \pmod 4 \end{aligned}\right\} \tag{4.23}$$

$$S_o^p = S_1^p = R^m = [S_o, S_i] = [S_1, S_{i+1}] = 1 \tag{4.24}$$

$$S_n = S_o^{a_o} S_1^{a_1} \ldots S_{n-1}^{a_{n-1}}, \quad S_{n+1} = S_1^{a_o} S_2^{a_1} \ldots S_n^{a_{n-1}} \tag{4.25}$$

$$S_k = S_o^d S_i^e, \quad S_{k+1} = S_1^d S_{i+1}^e \tag{4.26}$$

where $S_{2j} = R^j S_o R^{-j}$ and $S_{2j+1} = R^j S_1 R^{-j}$, $m = (p^n-1)/2$ is $PSL(2,p^n)$. Moreover, such a trinomial always exists.

Proof

By Sinkov's results, we have that $PSL(2,p^n)$ can be presented on generators U, R, S_o, S_1 subject to the relations (4.1), (4.2), (4.3), (4.7), (4.8) and (4.6). By lemma 4.1, since x satisfies the trinomial we can add the relations (4.26). Using (4.24) and (4.26) we see that R, S_o, S_1 satisfy the relations of $K_p((p^n-1)/2,k,i)$ and so by the substitution test we have an epimorphism from $K_p((p^n-1)/2,k,i)$ onto $\langle R, S_o, S_1 \rangle$ under $a \longmapsto R$, $b_o \longmapsto S_o$, $b_1 \longmapsto S_1$. We know that in $K_p((p^n-1)/2,k,i)$ the relations $[b_o, b_j] = [b_1, b_{j'}] = 1$, $j = 1,2,\ldots,n-1$ and $j' = 2,3,\ldots,n-1$, are implicit. Hence the relations (4.24) and (4.26) imply the relations (4.2) and (4.3). These are therefore redundant and can be removed.

Since x is primitive in $GF(p^n)$, then every element is a power of x. In particular, $\exists k \in N$ such that $1 + x = x^k$. Since $1^2 \neq 0 \pmod p$, and since $(1, (p^n-1)/2) = 1$, then such a trinomial always exists. Therefore, for each n, there is a presentation for $PSL(2,p^n)$ of this form.

Corollary 4.7

If x is primitive in $GF(p^n)$ and satisfies an irreducible polynomial

$$x^n = d + ex^i$$

where i is an odd integer and $(i, (p^n-1)/2) = 1$, then the following is a presentation for $PSL(2,p^n)$:

$$\langle U, R, S_o, S_1 \mid R^{(p^n-1)/2} = S_o^p = S_1^p = U^3 = (UR)^2 = (US_o)^2 = 1,$$

$$[S_o,S_i] = [S_1,S_{i+1}] = 1,\ S_n = S_o^d S_i^e,\ S_{n+1} = S_1^d S_{i+1}^e \rangle$$

together with $(S_1RU)^3 = 1$ if $p^n \equiv 1 \pmod 4$, where $S_{2j} = R^j S_o R^{-j}$ and $S_{2j+1} = R^j S_1 R^{-j}$.

Proof

We first note that $d^2 \neq (e-1)^2 \pmod p$ or that $e^2 \neq (d-1)^2 \pmod p$. To see this, consider the two cases separately.

If n is odd, we require $d^2 \neq (e-1)^2 \pmod p$. Since y^n-d-ey^i is irreducible over GF(p), then 1 and -1 are not roots. So, $1-d-e \neq 0$ and $-1-d+e \neq 0$. So, $d \neq 1-e$ and $d \neq e-1$. Hence $d^2 \neq (1-e)^2$.

Similarly, if n is even, we know that 1 and -1 do not satisfy the trinomial. So, $1-d-e \neq 0$ and $1-d+e \neq 0$. That is, $e \neq 1-d$ and $e \neq d-1$. That is, $e^2 \neq (1-d)^2$.

Now, using the presentation in theorem 4.6, we see that the relations (4.25) and (4.26) are identical. Therefore, the relations (4.25) are redundant and can be removed.

Remark

Theorem 4.6 and corollary 4.7 have given us presentations for $PSL(2,p^n)$ in which the deficiency does not decrease with n. The deficiencies of these presentations are -9,-8,-7 or -6 depending on whether $p^n \equiv 1 \pmod 4$ and whether or not we can

find an irreducible primitive trinomial of degree n satisfying the required conditions. It is not known, in general, if a primitive irreducible trinomial of arbitrary degree exists.

Theorem 4.8

If x is a primitive element of $GF(p^n)$ and satisfies the trinomial

$$x^k = d + ex^i$$

where $d^2 \neq (1-e)^2$ for k odd, $e^2 \neq (1-d)^2$ for k even, i is an odd integer with $(i, (p^n-1)/2) = 1$, and if the trinomial has precisely n roots in $GF(p^n)$, then $PSL(2,p^n)$ is isomorphic with

$$\langle U, R, S_o, S_1 \mid U^3 = R^m = (UR)^2 = (US_o)^2 = S_o^p = S_1^p = [S_o,S_i] = 1,$$

$$[S_1,S_{i+1}] = 1,\ S_k = S_o^d S_i^e,\ S_{k+1} = S_1^d S_{i+1}^e \rangle$$

with $(S_1RU)^3 = 1$ if $p^n \equiv 1 \pmod 4$, where $S_{2j} = R^j S_o R^{-j}$, $S_{2j+1} = R^j S_1 R^{-j}$ and $m = (p^n-1)/2$.

Proof

Let K be the above group. By theorem 4.6 and Von Dyck's theorem, if we add the relations

$$S_o^{a_o} S_1^{a_1} \ldots S_{n-1}^{a_{n-1}} S_n^{-1} = 1 \tag{4.27}$$

$$S_1^{a_o} S_2^{a_1} \ldots S_n^{a_{n-1}} S_{n+1}^{-1} = 1 \tag{4.28}$$

to K, we obtain $PSL(2,p^n)$. Let $H = \langle R, S_o, S_1 \rangle \leq K$, and $N \trianglelefteq K$ be such that $K/N \cong PSL(2,p^n)$. The isomorphism from the presentation in theorem 4.6 to $PSL(2,p^n)$ is satisfied by:

$$U \longleftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},\ R \longleftrightarrow \begin{pmatrix} x & x^{-1} \\ 0 & x^{-1} \end{pmatrix},\ S_o \longleftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ S_1 \longleftrightarrow \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

using Todd's results.

There is an epimorphism ϕ: $K \longrightarrow PSL(2,p^n)$ with $\text{Ker } \phi = N$.

Now HN/N is just the subgroup of upper triangular matrices, generated by $\begin{pmatrix} x & x^{-1} \\ 0 & x^{-1} \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, which as we saw in chapter one, has order $p^n(p^n-1)/2$. Suppose we can show $|H| = p^n(p^n-1)/2$. Then since $HN/N \equiv H/(H \cap N)$ we have $H \cap N = 1$. But clearly

$$S_o^{a_o} S_1^{a_1} \dots S_{n-1}^{a_{n-1}} S_n^{-1}, S_1^{a_o} S_2^{a_1} \dots S_n^{a_{n-1}} S_{n+1}^{-1} \in H \cap N,$$

and so the relations (4.27), (4.28) hold in K, showing that $K \equiv PSL(2,p^n)$. Now H is an epimorphic image of $K_p((p^n-1)/2,k,i)$ using the substitution test and the mapping

$$a \longmapsto R,\ b_o \longmapsto S_o,\ b_1 \longmapsto S_1 .$$

Therefore $|H| \leq |K_p((p^n-1)/2,k,i)|$. Now, $|K_p((p^n-1)/2,k,i)| = (p^n-1)/2.\,|K'((p^n-1)/2,k,i)|$ by theorems 4.3 and 4.5.

For k even, k = 2m, we have shown in theorem 4.3 that $K'((p^n-1)/2,k,i)$ is isomorphic with the abelian group

$$\langle y_j, z_j \mid y_j^p = z_j^p = [y_j,z_{j+r}] = [y_{j+r+1},z_j] = 1,\ y_{j+m} = y_j^d z_{j+r}^e,\ z_{j+m} = z_j^d y_{j+r+1}^e \rangle$$

where $j = 1,2,\dots,(p^n-1)/2$, $r = (i-1)/2$.

For k odd, k = 2m+1, by theorem 4.5, $K'((p^n-1)/2,k,i)$ is isomorphic with the abelian group

$$\langle y_j, z_j \mid y_j^p = z_j^p = [y_j,z_{j+r}] = [z_j,y_{j+r+1}] = 1,\ z_{j+m} = y_j^d z_{j+r}^e,\ y_{j+m+1} = z_j^d y_{j+r+1}^e \rangle$$

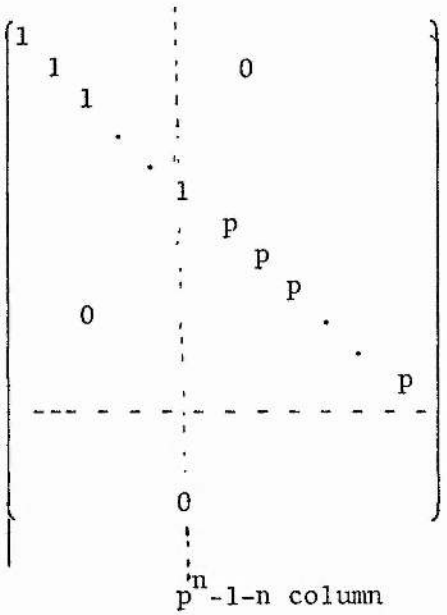
where $r = (i-1)/2$, $j = 1,2,\dots,(p^n-1)/2$.

The relation matrix for these groups takes the form

$$\begin{pmatrix} M_1 \\ M_2 \end{pmatrix}$$

where M_1 is a $(p^n-1)\times(p^n-1)$ diagonal matrix $(p,p,\dots,p)$ formed by

the relations $y_j^p = z_j^p = 1$. Under the rule that the even columns contain powers of y_j and the odd columns contain powers of z_j, M_2 is a circulant $(p^n-1)x(p^n-1)$ matrix. For k even, the first row is zero except in the first, $2(r+1)^{th}$ and $(2m+1)^{th}$ position where the entries are d, e and -1, respectively. For k odd, the first row of M_2 is zero except in the first $2(r+1)^{th}$ and $2(m+1)^{th}$ positions, where the entries are d, e and -1, respectively. For any k it follows from lemma 1.31 that the rank of M_2 is p^n-1-n, since the trinomial has precisely n roots in $GF(p^n)$. We perform elementary row and column operations on M_2 working mod p since, at any stage, we may subtract a multiple of any row of M_1. By the results of chapter one, M_2 can be reduced to a diagonal matrix $(d_1, d_2, \ldots, d_{p^n-1-n}, 0, 0, \ldots, 0)$ where each d_i satisfies $(d_i, p) = 1$ and $d_i \mid d_{i+1}$. Performing elementary row operations, the relation matrix becomes



p^n-1-n column

Hence $|K'_p((p^n-1)/2,k,i)|$ is p^n and so $|H| \leq p^n(p^n-1)/2$ and our theorem is proved.

It is quite difficult to reduce these presentations for $PSL(2,p^n)$. However, further reduction does occur when $p^n \equiv -1$

(mod 4). We note that in this case the relation $(S_1RU)^3 = 1$ may be dropped.

Lemma 4.9

$p^n \equiv -1 \pmod 4 \Leftrightarrow p \equiv -1 \pmod 4$ and n is odd.

Proof

If $p \equiv 1 \pmod 4$, then $p^n \equiv 1 \pmod 4$ for any n. If $p \equiv -1 \pmod 4$, then $p^{2n} \equiv 1 \pmod 4$ and so we require n to be odd, and $p \equiv -1 \pmod 4$.

Lemma 4.10

If $p^n \equiv -1 \pmod 4$, then in the above presentations for $PSL(2,p^n)$,

$$S_1 = R^{(p^n+1)/4} S_o^{-1} R^{-(p^n+1)/4}.$$

Proof

Since $p^n+1 \equiv 0 \pmod 4$, then $4 \nmid p^n-1$ and so $2 \nmid \frac{p^n-1}{2}$. That is $(p^n-1)/2$ is odd. Since x is primitive in $GF(p^n)$, then $x^{(p^n-1)/2} = -1$ which implies $x^{(p^n+1)/2} = -x$. Therefore, $-x = x^{2r}$ for some r. Now using the matrices corresponding to R, S_o and S_1 we see that

$$R^k S_o R^{-k} = \begin{pmatrix} 1 & x^{2k} \\ 0 & 1 \end{pmatrix}.$$

In particular, with $k = (p^n+1)/4$, we have:

$$R^k S_o R^{-k} = \begin{pmatrix} 1 & x^{(p^n+1)/2} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} = S_1^{-1}.$$

Finally,

$$S_1 = R^{(p^n+1)/4} S_o^{-1} R^{-(p^n+1)/4}.$$

This is the key to reducing our presentations, as the next result shows.

Theorem 4.11

Let x be a primitive element of $GF(p^n)$ satisfying the irreducible polynomial

$$m(y) = y^n - \sum_{i=0}^{n-1} a_i y^i,$$

that is, $m(x) = 0$, and let k be such that $1+x = x^k$ in $GF(p^n)$. If $p^n \equiv -1 \pmod 4$, then $PSL(2,p^n)$ can be presented as:

$$\langle U, R, S \mid U^3 = (UR)^2 = (US)^2 = R^m = S^p = S^{m(y)} = [S, R^t S R^{-t}] = 1, \quad R^r S R^{-r} = w \rangle$$

where $m = (p^n-1)/2$, $t = (p^n+1)/4$,

$r = (k-1)/2$, $w = S R^{-t} S^{-1} R^t$ if k is odd,

$r = k/2$, $w = S R^t S^{-1} R^{-t}$ if k is even,

and by $S^{m(y)}$ we mean the word

$$S_o^{a_o} S_1^{a_1} \cdots S_{n-1}^{a_{n-1}} S_n^{-1}$$

where $S_{2j} = R^j S R^{-j}$ and $S_{2j+1} = R^{j+t} S^{-1} R^{-j-t}$.

Proof

Using the presentation from theorem 4.6, the defining relations for $PSL(2,p^n)$ are:

$$U^3 = (UR)^2 = (US_o)^2 = R^m = S_o^p = 1 \tag{4.29}$$

$$S_1^p = [S_o, S_1] = [S_1, RS_oR^{-1}] = 1 \tag{4.30}$$

$$S_k = S_o S_1, \quad S_{k+1} = S_1 R S_o R^{-1} \tag{4.31}$$

$$S_n = S_o^{a_o} S_1^{a_1} \cdots S_{n-1}^{a_{n-1}} \tag{4.32}$$

$$S_{n+1} = S_1^{a_o} S_2^{a_1} \cdots S_n^{a_{n-1}} \tag{4.33}$$

Since $p^n \equiv -1 \pmod 4$, by lemma 4.10 we can add on the relation

$$S_1 = R^t S_o^{-1} R^{-t} \tag{4.34}$$

We shall show (4.33) is redundant. First, we note that

$$R^t S_{2j} R^{-t} = R^{t+j} S_o R^{-t-j} = R^j S_1^{-1} R^{-j} = S_{2j+1}^{-1}.$$

Also, $R^t S_{2j+1} R^{-t} = R^t\, R^j S_1 R^{-j}\, R^{-t} = R^{j+2t} S_o^{-1} R^{-j-2t}$.

Since $2t = (p^n+1)/2 = (p^n-1)/2 + 1$, we have $R^{2t} = R^m R = R$.

So, $R^t S_{2j+1} R^{-t} = R^{j+1} S_o^{-1} R^{-j-1} = S_{2j+2}^{-1}$. Therefore, using (4.32) we have:

$$\begin{aligned} R^{1-t} S_n R^{t-1} &= R^{1-t} S_o^{a_o}\, S_1^{a_1} \ldots S_{n-1}^{a_{n-1}} R^{t-1} \\ &= R^t S_o^{a_o}\, S_1^{a_1} \ldots S_{n-1}^{a_{n-1}} R^{t-1} \quad (\text{since } R^{2t} = R) \\ &= S_1^{-a_o}\, R^t S_1^{a_1}\, S_2^{a_2} \ldots S_{n-1}^{a_{n-1}}\, R^{t-1} \\ &= S_1^{-a_o} S_2^{-a_1}\, S_3^{-a_2} \ldots S_n^{-a_{n-1}}\, R^{2t-1} \\ &= S_1^{-a_o}\, S_2^{-a_1}\, S_3^{-a_2} \ldots S_n^{-a_{n-1}}. \end{aligned}$$

But, $R^{1-t} S_n R^{t-1} = R^{1-t} R^{(n-1)/2} S_1 R^{-(n-1)/2} R^{t-1}$ (since n is odd)

$$\begin{aligned} &= R^{(n+1)/2-t} R^t S_o^{-1} R^{-t} R^{-(n+1)/2} R^t \\ &= R^{(n+1)/2}\, S_o^{-1} R^{-(n+1)/2} \\ &= S_{n+1}^{-1}. \end{aligned}$$

Hence,

$$S_{n+1} = S_n^{a_{n-1}}\, S_{n-1}^{a_{n-2}} \ldots S_2^{a_1}\, S_1^{a_o}.$$

That is, $S_{n+1} = S_1^{a_o}\, S_2^{a_1}\, S_3^{a_2} \ldots S_n^{a_{n-1}}$

since these terms commute, and the fact that they commute is only dependent on the trinomial relations (4.31). But this is (4.33) and is therefore redundant as it is implied by the other relations. To complete the proof, we consider the cases k even and k odd separately.

Case 1 $k = 2r$: On replacing S_1 in the remaining relations by

using (4.34) and writing S_o as S, the defining relations become:

$$U^3 = (UR)^2 = (US)^2 = R^m = S^p = 1 \tag{4.35}$$

$$R^t S^{-p} R^{-t} = 1 \tag{4.36}$$

$$[S, R^t S R^{-t}] = 1 \tag{4.37}$$

$$[R^t S^{-1} R^{-t}, RSR^{-1}] = 1 \tag{4.38}$$

$$R^r S R^{-r} = S R^t S^{-1} R^{-t} \tag{4.39}$$

$$R^{r+t} S^{-1} R^{-r-t} = R^t S^{-1} R^{-t} RSR^{-1} \tag{4.40}$$

$$S^{m(x)} = 1 \tag{4.41}$$

where $S^{m(x)} = 1$ is the relation (4.32) with S_1 replaced. Clearly, (4.36) is redundant. Now,

$$R^t S^{-1} R^{-t} RSR^{-1} R^t S^{-1} R^{-t} RS^{-1} R^{-1}$$

$$= R^t SR^{-t} R^t SR^{-t} R^{r+t} S^{-1} R^{-r-t} R^t S^{-1} R^{-t} R^{r+t} SR^{-r-t} R^t S^{-1} R^{-t}$$

$$= R^t S^2 R^r S^{-1} R^{-r} S^{-1} R^r SR^{-r} S^{-1} R^{-t}$$

$$= R^t S^2 R^t SR^{-t} S^{-1} S^{-1} SR^t S^{-1} R^{-t} S^{-1} R^{-t} \quad \text{(using (4.39))}$$

$$= R^t S^2 (R^t SR^{-t}) S^{-1} (R^t S^{-1} R^{-t}) S^{-1} R^{-t}$$

$$= R^t SR^t SR^{-t} R^t S^{-1} R^{-t} S^{-1} R^{-t} \quad \text{(using (4.37))}$$

$$= 1.$$

Therefore, the relation (4.38) is redundant.

Also,

$$R^{r+t} S^{-1} R^{-r-t} = R^t R^r S^{-1} R^{-r} R^{-t}$$

$$= R^t R^t SR^{-t} S^{-1} R^{-t} \quad \text{(using (4.39))}$$

$$= R^t S^{-1} R^t SR^{-2t} \quad \text{(using (4.37))}$$

$$= R^t S^{-1} R^{-t} RSR^{-1} \quad \text{(since } R^{2t} = R\text{)}$$

Therefore, (4.40) is redundant, proving the theorem for k even.

Case 2 k = 2r+1 : On replacing S_1, our relations are (4.35), (4.36), (4.37), (4.38), (4.41) and

$$R^{r+t}S^{-1}R^{-r-t} = SR^{t}S^{-1}R^{-t} \tag{4.42}$$

$$R^{r+1}SR^{-1-r} = R^{t}S^{-1}R^{-t}RSR^{-1} \ . \tag{4.43}$$

Again (4.36) is clearly redundant.

$$\begin{aligned}
&R^{t}SR^{-t}RSR^{-1}R^{t}S^{-1}R^{-t}RS^{-1}R^{-1} \\
&\quad = R^{t}SR^{-t}R^{t}SR^{-t}R^{r+1}SR^{-1-r}R^{t}S^{-1}R^{-t}R^{1+r}S^{-1}R^{-1-r}R^{t}S^{-1}R^{-t} \\
&\quad = R^{t}S^{2}R^{r+1-t}SR^{-1-r+t}S^{-1}R^{1+r-t}S^{-1}R^{t-1-r}S^{-1}R^{-t} \\
&\quad = R^{t}S^{2}R^{r+t}SR^{-r-t}S^{-1}R^{r+t}S^{-1}R^{-r-t}S^{-1}R^{-t} \\
&\quad = R^{t}S^{2}R^{t}SR^{-t}S^{-1}S^{-1}SR^{t}S^{-1}R^{-t}S^{-1}R^{-t} \\
&\quad = R^{t}SR^{t}SR^{-t}R^{t}S^{-1}R^{-t}S^{-1}R^{-t} \\
&\quad = 1.
\end{aligned}$$

Hence (4.38) is redundant. By (4.42) we have,

$$\begin{aligned}
&R^{r}S^{-1}R^{-r} = R^{-t}SR^{t}S^{-1} \\
\Rightarrow\ &R^{r+1}S^{-1}R^{-1-r} = R^{1-t}SR^{t}S^{-1}R^{-1} \\
\Rightarrow\ &R^{r+1}SR^{-1-r} = RSR^{-t}SR^{t-1} \\
&\qquad = R^{t}R^{t}SR^{-t}SR^{t-1} \quad (\text{since } R^{2t} = R) \\
&\qquad = R^{t}SR^{t}SR^{-1} \qquad (\text{using (4.37)}) \\
&\qquad = R^{t}SR^{-t}RSR^{-1},
\end{aligned}$$

and so (4.43) is redundant.

Finally, we can write (4.42) as,

$$R^{r}S^{-1}R^{-r} = R^{-t}SR^{t}S^{-1}$$

That is, $$R^{r}SR^{-r} = SR^{-t}S^{-1}R^{t}$$

which proves the theorem for k odd.

Corollary 4.12

If x is primitive in $GF(p^n)$, $p^n \equiv -1 \pmod 4$, and satisfies the trinomial $y^k - 1 - y$, and if the trinomial has precisely n roots

in $GF(p^n)$, then $PSL(2,p^n)$ is isomorphic with

$$\langle U,R,S \mid U^3 = (UR)^2 = (US)^2 = R^m = S^p = [S,R^tSR^{-t}] = 1,$$
$$R^rSR^{-r} = w \rangle$$

where $m = (p^n-1)/2$, $t = (p^n+1)/4$,

$r = k/2$, $w = SR^tS^{-1}R^{-t}$ if k is even,

$r = (k-1)/2$, $w = SR^{-t}S^{-1}R^t$ if k is odd.

Proof

By theorem 4.8, the relation $S^{m(x)} = 1$ is redundant in the above theorem.

Example 4.13

The polynomial x^3-x^2-2x-2 is irreducible over GF(3) and is satisfied by a primitive element of GF(27). The Sinkov presentation for PSL(2,27) is then

$$\langle U, R, S_o, S_1 \mid U^3 = (UR)^2 = (US_o)^2 = R^{13} = S_o^3 = S_1^3 = [S_o,S_1] = 1,$$
$$[S_o,RS_oR^{-1}] = [S_1,RS_oR^{-1}] = 1,$$
$$RS_1R^{-1} = S_o^2S_1^2RS_oR^{-1},\ R^2S_oR^{-2} = S_1^2RS_o^2R^{-1}RS_1R^{-1} \rangle \quad (4.44)$$

The primitive element also satisfies

$$1+x = x^{19}.$$

Therefore, by theorem 4.6 we have as a presentation for PSL(2,27)

$$\langle U, R, S_o,S_1 \mid U^3 = (UR)^2 = (US_o)^2 = S_o^3 = S_1^3 = R^{13} = [S_o,S_1] = 1$$
$$[S_1,RS_oR^{-1}] = 1,\ R^9S_1R^{-9} = S_oS_1,\ R^{10}S_oR^{-10} = S_1RS_oR^{-1},$$
$$RS_1R^{-1} = S_o^2S_1^2RS_oR^{-1},\ R^2S_oR^{-2} = S_1^2RS_o^2R^{-1}RS_oR^{-1} \rangle \quad (4.45)$$

Unfortunately, the deficiency is greater in (4.44) than in the

above presentation. However, for larger n, theorem 4.6 guarantees a presentation with less defining relations.

Now $27 \equiv -1 \pmod 4$, $k = 19$ is odd. $(27+1)/4 = 7$.

By theorem 4.11, the presentation (4.45) reduces to

$$\langle U, R, S \mid U^3 = (UR)^2 = (US)^2 = R^{13} = S^3 = [S,R^7SR^{-7}] = 1,$$
$$R^8S^{-1}R^{-8} = S^2R^7S^{-2}R^{-6}SR^{-1},\ R^9SR^{-9} = SR^{-7}S^{-1}R^7 \rangle \quad (4.46)$$

which is a deficiency -5 presentation for PSL(2,27). Now the trinomial $x^{19}-1-x$ has exactly three roots in GF(27). So, by corollary 4.12, (4.46) becomes,

$$\langle U,R,S \mid U^3 = (UR)^2 = (US)^2 = R^{13} = S^3 = [S,R^7SR^{-7}] = 1,$$
$$R^9SR^{-9} = SR^{-7}S^{-1}R^7 \rangle$$

We can reduce the exponents of R in the last relation as follows.

$$R^9SR^{-9} = SR^{-7}S^{-1}R^7$$
$$\Leftrightarrow R^{16}SR^{-16} = R^7SR^{-7}S^{-1}$$
$$\Leftrightarrow R^3SR^{-3} = R^7SR^{-7}S^{-1}.$$

Theorem 4.14

With the notation of theorem 4.11, $PSL(2,p^n)$, $p^n \equiv -1 \pmod 4$, has a deficiency -4 presentation

$$\langle U, R, S \mid U^3 = (UR)^2 = (US)^2 = S^{m(x)} = [S,R^tSR^{-t}] = 1,\ R^m = S^p$$
$$R^rSR^{-r} = w \rangle$$

Proof

Since $R^m = S^p$, then $[R^m,S] = 1$ and $[S^p,R] = 1$. When k is even, the last relation is

$$R^rSR^{-r} = SR^tS^{-1}R^{-t}.$$

Now, $S^p = R^rS^pR^{-r}$ and so,

$$R^rS^pR^{-r} = S^p = (SR^tS^{-1}R^{-t})^p = S^pR^tS^{-p}R^{-t} = 1,$$

since $[S,R^tSR^{-t}] = 1$. Hence, $R^m = S^p = 1$.

When k is odd, the last relation is,

$$R^rSR^{-r} = SR^{-t}S^{-1}R^t.$$

Therefore,

$$R^{r+t}SR^{-r-t} = R^tSR^{-t}S^{-1}.$$

Raising this to the power p gives

$$R^{r+t}S^pR^{-r-t} = R^tS^pR^{-t}S^{-p} = 1,$$

since $[S,R^tSR^{-t}] = 1$. So, again we have $S^p = R^m = 1$. By theorem 4.11, in both cases, we deduce the group presented above is $PSL(2,p^n)$.

There is the inevitable corollary to this.

Corollary 4.15

If $1+x = x^k$ has precisely n roots in $GF(p^n)$, then $PSL(2,p^n)$ has a deficiency -3 presentation,

$$\langle U, R, S \mid U^3 = (UR)^2 = (US)^2 = [S,R^tSR^{-t}] = 1,\ R^m = S^p, R^rSR^{-r} = w \rangle$$

Proof

Follows from corollary 4.12 and theorem 4.14.

Corollary 4.7 provides a presentation for $PSL(2,p^n)$ when the irreducible polynomial is a trinomial y^n-d-ey^i, and satisfied by a primitive element, x, of $GF(p^n)$. We can reduce this presentation even more when $p^n \equiv -1 \pmod 4$.

Theorem 4.16

Let x be a primitive element of $GF(p^n)$, $p^n \equiv -1 \pmod 4$. Suppose x is a root of an irreducible trinomial

$$y^n - d - ey^i$$

where $(i,(p^n-1)/2) = 1$. Then $PSL(2,p^n)$ can be presented as

$$\langle U, R, S \mid U^3 = (UR)^2 = (US)^2 = R^m = S^p = [S,R^{j+t}SR^{-j-t}] = 1,$$
$$R^{q+t}S^{-1}R^{-q-t} = S^{d}R^{t+j}S^{-e}R^{-j-t} \rangle$$

where $m = (p^n-1)/2$, $t = (p^n+1)/4$, $j = (i-1)/2$ and $q = (n-1)/2$.

Proof

By corollary 4.7, $PSL(2,p^n)$ is generated by U, R, S_o and S_1 subject to the relations:

$$R^m = S_o^p = U^3 = (UR)^2 = (US_o)^2 = 1 \tag{4.47}$$

$$[S_o,R^jS_1R^{-j}] = [S_1,R^{j+1}S_oR^{-1-j}] = S_1^p = 1$$

$$R^qS_1R^{-q} = S_o^d R^jS_1^e R^{-j}$$

$$R^{q+1} S_oR^{-q-1} = S_1^dR^{j+1} S_o R^{-1-j}.$$

By lemma 4.10, we can add the relation

$$S_1 = R^tS_o^{-1}R^{-t} . \tag{4.48}$$

We use (4.48) to eliminate S_1. On writing S_o as S, the relations (4.47) together with

$$[S,R^{j+t}SR^{-j-t}] = 1 \tag{4.49}$$

$$R^tS^{-p}R^{-t} = 1 \tag{4.50}$$

$$[R^tS^{-1}R^{-t},R^{j+1}SR^{-1-j}] = 1 \tag{4.51}$$

$$R^{q+t}S^{-1}R^{-q-t} = S^dR^{j+t}S^{-e}R^{-j-t} \tag{4.52}$$

$$R^{q+1}SR^{-q-1} = R^tS^{-d}R^{-t}R^{j+1}S^eR^{-j-1} \tag{4.53}$$

define $PSL(2,p^n)$.

Clearly, (4.50) is redundant. Now,

$$R^tSR^{-t}R^{j+1}S^eR^{-1-j}R^tS^{-1}R^{-t}R^{j+1}S^{-e}R^{-1-j}$$

$$= R^tSR^{-t}R^tS^dR^{-t}R^{q+1}SR^{-1-q}R^tS^{-1}R^{-t}R^{q+1}S^{-1}R^{-1-q}R^tS^{-d}R^{-t}$$

$$= R^tS^{1+d}R^{1-2t}R^{q+t}SR^{-q-t}R^{-1+2t}S^{-1}R^{1-2t}R^{q+t}S^{-1}R^{-q-t}R^{2t-1}S^{-d}R^{-t}$$

$$= R^tS^{1+d}R^{j+t}S^eR^{-j-t}S^{-d}S^{-1}S^dR^{j+t}S^{-e}R^{-j-t}S^{-d}R^{-t} \quad \text{(since } R^{2t} = R\text{)}$$

$$= R^{t}S^{d}R^{j+t}S^{e}R^{-j-t}R^{j+t}S^{-e}R^{-j-t}S^{-d}R^{-t} \quad \text{(using (4.49))}$$

$$= 1.$$

So, $[R^{t}SR^{-t}, R^{j+1}S^{e}R^{-1-j}] = 1$ is implied by the other relations. Since $(e,p) = 1$, then this implies

$$[R^{t}SR^{-t}, R^{j+1}SR^{-1-j}] = 1.$$

Hence (4.51) is redundant and is removed since it is a consequence of the other relations. From (4.52) we have,

$$R^{q}S^{-1}R^{-q} = R^{-t}S^{d}R^{j+t}S^{-e}R^{-j}$$

$$\Rightarrow R^{q+1}S^{-1}R^{-q-1} = R^{1-t}S^{d}R^{j+t}S^{-e}R^{-j-1}$$

$$\Rightarrow R^{q+1}SR^{-q-1} = R^{1+j}S^{e}R^{-j-t}S^{-d}R^{t-1}$$

$$= R^{1-t}R^{j+t}S^{e}R^{-j-t}S^{-d}R^{t-1}$$

$$= R^{1-t}S^{-d}R^{j+t}S^{e}R^{-j-1} \quad \text{(using (4.49))}$$

$$= R^{t}S^{-d}R^{-t}R^{j+1}S^{e}R^{-1-j} \quad \text{(since } R^{2t} = R\text{)}.$$

But this is (4.53). Therefore, (4.53) is redundant and the proof is complete.

Corollary 4.17

With the notation of theorem 4.16,

$$G = \langle U, R, S \mid U^{3} = (US)^{2} = [S, R^{j+t}SR^{-j-t}] = 1,\ S^{p} = R^{m} = (UR)^{2},$$

$$R^{q+t}S^{-1}R^{-q-t} = S^{d}R^{j+t}S^{-e}R^{-j-t} \rangle$$

is $PSL(2,p^{n})$, provided $d-e+1$ is odd and either $(2p-2m-pm,3) = 1$ or $(d-e+1,3) = 1$.

Proof

We evaluate $|G/G'|$. The relation matrix is

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & m & -p \\ 2 & 2 & -p \\ 2 & 0 & 2 \\ 0 & 0 & d-e+1 \end{pmatrix}$$

Let d+1-e = c. We perform a series of row operations on the relation matrix, which becomes

$$\begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & -p+(p+2)(m+1)/2 \\ 0 & 0 & 2p-2m-mp \\ 0 & 0 & 6 \\ 0 & 0 & c \end{pmatrix}$$

2p-2m-mp is odd, and if it is coprime to 3, then there is a $k \in \mathbb{Z}$ with 2p-2m-mp = 6k+r, where r = 1 or 5. In this case, the last three rows reduce to

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 6 \\ 0 & 0 & c \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & 0 & 5 \\ 0 & 0 & 6 \\ 0 & 0 & c \end{pmatrix}$$

In both cases, the last three rows reduce to

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

This now shows that G = G'.

If (2p-2m-mp,3) = 3, then (c,3) = 1, and a similar argument shows that in this case, G = G', and so G is perfect.

Let $A = \langle S^p \rangle$. $A \leq G' = G$. $A \leq Z(G)$ for S^p commutes with S, R and UR and these three clearly generate G, showing $S^p \in Z(G)$. Also, by the previous theorem, $G/A \cong PSL(2,p^n)$. G is a stem extension of $PSL(2,p^n)$ and so by theorem 1.19 is either $PSL(2,p^n)$ or $SL(2,p^n)$. Hence, $Z(G) = 1$ or C_2. Therefore, either $S^p = 1$ or

$S^{2p} = 1$. If $S^p = 1$, then G is $PSL(2,p^n)$ and we are finished. Assume $S^{2p} = 1$.

$$R^{q+t}S^{-1}R^{-q-t} = S^{d}R^{j+t}S^{-e}R^{-j-t}$$

Raising this to the power p, and using $[S,R^{j+t}SR^{-j-t}] = 1$, we see that

$$R^{q+t}S^{-p}R^{-q-t} = S^{dp}R^{j+t}S^{-ep}R^{-j-t}.$$

That is, $S^{pc} = 1$ since S^p is central. But c is odd, and since $S^{2p} = 1$, we deduce that $S^p = 1$. Therefore, $G \cong PSL(2,p^n)$.

Remarks

If $c = d+1-e$ is even, then we can replace $-e$ by $p-e$, or d by $d-p$ in the above presentation and set $c' = d+1-e\pm p$, which is odd. We then require $(c',3) = 1$ if $(2p-2m-mp,3) \neq 1$.

Example 4.18

The trinomial x^3-2-x is irreducible over GF(3) and satisfied by a primitive element of GF(27). Therefore, from theorem 4.16 with $i = 1$, $d = 2$, $e = 1$ and $n = 3$, the following is a presentation for PSL(2,27).

$$\langle U, R, S \mid U^3 = (UR)^2 = (US)^2 = R^{13} = S^3 = [S,R^7SR^{-7}] = 1,$$
$$R^8S^{-1}R^{-8} = S^2R^7S^{-1}R^{-7} \rangle$$

Now $d+1-e = 2$ and so we cannot apply corollary 4.17 directly. But since $S^3 = 1$, we can write the last relation as

$$R^8S^{-1}R^{-8} = S^{-1}R^7S^{-1}R^{-7}.$$

Now, with $d = -1$, we have $(d+1-e,2) = (-1,2) = 1$. Also $6-26-39 = -59$ is coprime to 3. Therefore, a deficiency -3 presentation for PSL(2,27) is

$$\langle U, R, S \mid U^3 = (US)^2 = [S,R^7SR^{-7}] = 1,\ R^8S^{-1}R^{-8} = S^{-1}R^7S^{-1}R^{-7},$$
$$(UR)^2 = R^{13} = S^3 \rangle$$

As with $SL(2,2^n)$, it is often the case that using an irreducible polynomial, which is not satisfied by a primitive element of $GF(p^n)$, we obtain a presentation for $PSL(2,p^n)$. To illustrate this, consider the following example.

Example 4.19

The polynomial y^3-2 is irreducible over GF(7). Let x be a root, so that $x^3 = 2$. Now $x^9 = 2^3 = 1 \pmod 7$. Consider the group G generated by U, R, S_o, S_1 subject to the relations:

$$U^3 = R^9 = (US_o)^2 = S_o^7 = S_1^7 = [S_o,S_1] = [S_1,RS_oR^{-1}] = (UR)^2 = 1,$$

$$RS_1R^{-1} = S_o^2,\ R^2S_oR^{-2} = S_1^2 .$$

This is the 'Sinkov' presentation using the above polynomial. Using COSET, the index of $H = \langle R,S_o,S_1 \rangle$ in G is 6536. Also, using COSET, the order of

$$\overline{H} = \langle R, S_o, S_1 \mid R^9 = S_o^7 = S_1^7 = [S_o,S_1] = [S_1,RS_oR^{-1}] = 1,$$

$$RS_1R^{-1} = S_o^2,\ R^2S_oR^{-2} = S_1^2 \rangle$$

is 3087. Clearly $|\overline{H}| \geq |H|$ and so $|G| \leq 3087.6536 = |PSL(2,7^3)|$. G has $PSL(2,7^3)$ as a homomorphic image, since the matrices

$$U' = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},\ R' = \begin{pmatrix} x & x^{-1} \\ 0 & x^{-1} \end{pmatrix},\ S_o' = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ S_1' = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

satisfy the relations of G, under the obvious correspondence. These matrices also generate $PSL(2,7^3)$. Therefore, the above is a presentation for $PSL(2,7^3)$. In fact, we can deduce a deficiency -2 presentation from this.

As $S_1 = R^{-1}S_o^2R$, we can replace S_1 in terms of R and S_o. Also, since (2,7) = 1, and S_1 is a conjugate of S_o^2, the relation $S_1^7 = 1$, can be omitted. The defining relations become,

$$U^3 = R^9 = S^7 = (US)^2 = [S,R^{-1}S^2R] = [R^{-1}S^2R,RSR^{-1}] = (UR)^2 = 1,$$

and $R^3SR^{-3} = S^4$.

As S commutes with $R^{-1}S^2R$, then S commutes with powers of $R^{-1}S^2R$, and in particular with $R^{-1}SR$. So the relation $[S,R^{-1}SR] = 1$ holds in G. But this implies $[S,R^{-1}S^2R] = 1$. Therefore, we can replace $[S,R^{-1}S^2R] = 1$ by $[S,R^{-1}SR] = 1$. Similarly, we can replace $[R^{-1}S^2R, RSR^{-1}] = 1$ by the relation $[R^{-1}SR, RSR^{-1}] = 1$. But,

$$\begin{aligned} R^{-1}S^{-1}RRS^{-1}R^{-1}R^{-1}SRRSR^{-1} &= R^{-1}S^{-1}(R^2S^{-1}R^{-2})SR^2SR^{-1} \\ &= R^{-1}S^{-1}(R^{-1}S^{-4}R)SR^2SR^{-1} \\ &= R^{-2}S^{-4}R^3SR^{-1} \text{ (since } [S,R^{-1}SR] = 1) \\ &= RS^{-1}SR^{-1} = 1. \end{aligned}$$

So $[R^{-1}SR,RSR^{-1}] = 1$ is redundant.

At this point, it is convenient to change the generating set by $US = w$, $S = x$, $S^{-1}R = z$. The defining relations become:

$$(wx)^3 = x^7 = (wz)^2 = w^2 = 1$$

$$[x,z^{-1}xz] = 1 \tag{4.54}$$

$$(xz)^9 = 1 \tag{4.55}$$

$$(xz)^3x(xz)^{-3} = x^4 \tag{4.56}$$

Now, $x^{-1}z^{-1}x^{-1}zxz^{-1}xz = 1 \Leftrightarrow zx^{-1}z^{-1}x^{-1}zxz^{-1}x = 1$. That is,

$$[x,\ zxz^{-1}] = 1. \tag{4.57}$$

So we can replace (4.54) by (4.57).

$$\begin{aligned} & x\,z\,x\,z\,x\,z\,x\,z^{-1}x^{-1}z^{-1}x^{-1}z^{-1}x^{-1} = x^4 \\ \Leftrightarrow\ & z\,x\,z\,x\,z\,x\,z^{-1}x^{-1}z^{-1}x^{-1}z^{-1} = x^4 \\ \Leftrightarrow\ & z\,x\,z^2x\,z^{-2}x^{-1}z^{-1} = x^4 \quad \text{(since } [x,zxz^{-1}] = 1) \\ \Leftrightarrow\ & z^2x\,z^{-2} = x^{-1}z^{-1}x^4z\,x = z^{-1}x^4\,z \\ \Leftrightarrow\ & z^3x\,z^{-3} = x^4. \end{aligned}$$

Also, $(xz)^9 = 1 \Leftrightarrow z^9 = 1$. For, $x\,z^2x\,z^{-2}x^{-1}z^2x^{-1}z^{-2} = x\,z^{-1}x^4zx^{-1}z^2x^{-1}z^{-2} = z^{-1}x^4z^3x^{-1}z^{-2} = z^{-1}z^3z^{-2} = 1$ showing that $[x,z^2x\,z^{-2}] = 1$.

Also, $z\ x\ z^{-1}z^2x\ z^{-2}z\ x^{-1}z^{-1}z^2x^{-1}z^{-2}$

$= z\ x\ z^{-1}z^{-1}x^4z\ z\ x^{-1}z^{-1}z^2x^{-1}z^{-2}$

$= z\ x\ z^{-2}x^4z^2x^{-1}z^{-1}z^2x^{-1}z^{-2}$

$= z^{-1}x^4z\ z^2x^{-1}z^{-2}$ (since $[x, z^2xz^{-2}] = 1$)

$= z^{-1}z^3z^{-2} = 1,$

showing that $[z\ x\ z^{-1},\ z^2x\ z^{-2}] = 1$.

Therefore,

$(xz)^9 = x\ z\ x\ z^{-1}z^2x\ z^{-2}z^3x\ z^{-3}z^4x\ z^{-4}z^5x\ z^{-5}z^6xz^{-6}z^7x\ z^{-7}z^8x\ z^{-8}z^9$

$= x\ z\ x\ z^{-1}z^2x\ z^{-2}x^4z\ x^4z^{-1}z^2x^4z^{-2}\ x^2z\ x^2z^{-1}z^2x^2z^{-2}z^9$

$= x^7z\ x\ z^{-1}z\ x^4z^{-1}z\ x^2z^{-1}z^2x\ z^{-2}z^2x^4z^{-2}z^2x^2z^{-2}z^9$

$= z^9$ (since $x^7 = 1$).

Therefore, we can replace $(xz)^9 = 1$ by $z^9 = 1$. (4.58)

Also, $z^3x\ z^{-3} = x^4 \Leftrightarrow z^{-3}x^4z^3 = x \Leftrightarrow z^{-3}x\ z^3 = x^2$.

Therefore, $PSL(2,7^3)$ can be presented as:

$\langle w, x, z \mid w^2 = (wx)^3 = x^7 = z^9 = (wz)^2 = [x, zxz^{-1}] = 1,$

$z^{-3}x\ z^3 = x^2 \rangle$

The relation $x^7 = 1$ is redundant, for

$z^{-3}x\ z^3 = x^2$

$\Rightarrow z^{-6}x\ z^6 = x^4$

$\Rightarrow z^{-9}x\ z^9 = x^8.$

That is, $x^7 = 1$. Finally,

$G = \langle w, x, z \mid w^2 = [x, zxz^{-1}] = 1,\ (wz)^2 = (wx)^3 = z^9,$

$z^{-3}x\ z^3 = x^2 \rangle$

is a presentation for $PSL(2,7^3)$. For, $z^9 \in Z(G)$ and it is easily checked that G is perfect. Also, $G/\langle z^9 \rangle \cong PSL(2,7^3)$. By theorem 1.19, G is $PSL(2,7^3)$ or $SL(2,7^3)$. Since $Z(SL(2,7^3)) = C_2$, then $z^{18} = 1$ if $G = SL(2,7^3)$. If $G = PSL(2,7^3)$ then $z^9 = 1$. In either case $z^{18} = 1$. Now $w\ z\ w = z^8 \Rightarrow w\ z^9 w = z^{72} \Rightarrow z^9 = z^{72} = 1$, since z^9 is central. Hence, G is $PSL(2,7^3)$ and the above is a

deficiency -2 presentation.

For $p^n \equiv 1 \pmod 4$ things are not so easy and it is difficult in general to reduce the presentation. Quite often, one can eliminate a generator and possibly one relation.

Example 4.20

The polynomial x^4-1-2x is irreducible over GF(3) and is satisfied by a primitive element of GF(81). We have, using corollary 4.7, the following presentation for PSL(2,81).

$$\langle U, R, S_o, S_1 \mid U^3 = R^{40} = S_o^3 = S_1^3 = (UR)^2 = (US_o)^2 = (S_1RU)^3 = 1,$$

$$[S_o,S_1] = [S_1,RS_oR^{-1}] = 1,\ R^2S_oR^{-2} = S_oS_1^2,$$

$$R^2S_1R^{-2} = S_1RS_o^2R^{-1} \rangle$$

Since $S_1^2 = S_1^{-1}$, we have $S_1 = R^2S_o^{-1}R^{-2}S_o$, using the tenth relation. So, $[S_o,S_1] = 1$ becomes $[S_o,R^2S_oR^{-2}S_o] = 1 \Leftrightarrow [S_o,R^2S_oR^{-2}] = 1$. $S_1^3 = 1$ becomes $(S_oR^2S_o^{-1}R^{-2})^3 = 1$. But this is redundant since $[S_o,R^2S_oR^{-2}] = 1$ and $S_o^3 = 1$. Therefore, our defining relations become (on replacing S_1 and writing S_o as S):

$$U^3 = R^{40} = S^3 = (US)^2 = (UR)^2 = [S,R^2SR^{-2}] = (R^2S^{-1}R^{-2}SRU)^3 = 1,$$

$$[R^2S^{-1}R^{-2}S,\ RSR^{-1}] = 1,\ R^4S^{-1}R^{-2}SR^{-2} = R^2S^{-1}R^{-2}SRS^2R^{-1}\ .$$

In the next chapter, we shall investigate presentations for the groups $PSL(2,p^2)$, where of course $p^2 \equiv 1 \pmod 4$.

Chapter V. Presentations for $PSL(2,p^2)$, p an odd prime.

Most of our presentations for $PSL(2,p^n)$ have used a primitive element of the field $GF(p^n)$. It is clear that we cannot use any element of the field (see examples following theorem 2.19). Under suitable circumstances we have shown that the condition can be weakened to using a non-primitive element.

In this chapter, we derive a presentation for $PSL(2,p^2)$ using an irreducible polynomial which is not satisfied by a primitive element of $GF(p^2)$. The proof of this involves ideas we have met before, such as X sets. This result extends the 'Todd-Sinkov' result for $PSL(2,p^2)$.

Finally, we give efficient presentations for $PSL(2,p^2)$, $p = 5$ and 7, and also (a little out of place) for $PSL(2,27)$.

We now obtain a presentation for $PSL(2,p^2)$ which does not use a primitive element of $GF(p^2)$. Throughout this chapter, we shall assume p is an odd prime.

Consider the polynomial

$$m_q(y) = y^2 - q$$

over GF(p), where q is a primitive element of GF(p).

Lemma 5.1

$m_q(y)$ is irreducible over GF(p).

Proof

Suppose $m_q(y)$ is not irreducible. Then, $\exists b \in GF(p)$ with $b^2 = q$. Then, $b^{p-1} = q^{(p-1)/2} = 1$ contradicting the fact that q is primitive in GF(p).

Let x be a root of $m_q(y)$, so that $x^2 = q$. Every element of $GF(p^2)$ can be expressed as $a + bx$, $a,b \in GF(p)$. The even powers of x correspond to elements of GF(p) and the odd powers of x correspond to elements of the form ax, $a \in GF(p)$. We note that $x^{2p-2} = 1$.

Definition 5.2

We define the groups $G_{q,p}$ as

$$\langle a, b, c, d \mid a^p = b^p = c^2 = (ac)^3 = (cd)^2 = d^{p-1} = (bdc)^3 = 1,$$
$$[a,b] = 1,\ d\,a\,d^{-1} = a^q,\ d\,b\,d^{-1} = b^q \rangle$$

We shall show that $G_{q,p}$ is isomorphic with $PSL(2,p^2)$.

Remark

This presentation is obtained from the 'Sinkov' presentation (using the polynomial $m_q(y)$ in 4.1-4.6) which is,

$$\langle U, R, S_o, S_1 \mid U^3 = R^{p-1} = S_o^p = S_1^p = (UR)^2 = (US_o)^2 = (S_1RU)^3 = 1,$$
$$[S_o,S_1] = 1,\ RS_oR^{-1} = S_o^q,\ RS_1R^{-1} = S_1^q \rangle$$

We have changed the generating set using the transformations

$$S_o = a,\ S_1 = b,\ US_o = c,\ S_o^{-1}R = d\ .$$

The proof that $(ad)^{p-1} = 1 \Leftrightarrow d^{p-1} = 1$ is similar to that used in chapter two, lemma 2.3.

In order to show $G_{q,p}$ is $PSL(2,p^2)$, we will make use of Beetham's presentation for $PSL(2,p^2)$ [1]. Beetham's presentation is:

$$\langle x_o, y_o, x_1, y_1 \mid x_i^p = y_i^p = [x_o,x_1] = [y_o,y_1] = (x_o^a x_1^b y_o^c y_1^d)^2 = 1 \rangle \qquad (5.1)$$

where $i = 0, 1$ and $(a + b\beta)(c + d\beta) = 1$, $\beta \in GF(p^2)^*$ is algebraic of degree 2 over $GF(p)$. The corresponding matrices can be taken to be:

$$x_o \longleftrightarrow \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad y_o \longleftrightarrow \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix}, \quad x_1 \longleftrightarrow \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix}, \quad y_1 \longleftrightarrow \begin{bmatrix} 1 & 0 \\ -2\beta & 1 \end{bmatrix}$$

It proves useful to put this in another form using Tietze transformations.

Theorem 5.3

$PSL(2,p^2)$ can be presented as

$$\langle x, y, w \mid x^p = y^p = w^2 = (wx)^3 = [x,y] = (x^a y^b w x^{2c} y^{2d} w)^2 = 1 \rangle \quad (5.2)$$

where $(a + b\beta)(c + d\beta) = 1$, $\beta \in GF(p^2)^*$ is algebraic of degree 2 over $GF(p)$.

Proof

We start with the presentation (5.1). The relation

$$(x_o\, y_o^{(p+1)/2}\, x_o)^2 = 1 \qquad (5.3)$$

holds in (5.1) since $(2 + 0\beta)((p+1)/2 + 0\beta) = 1$ in $GF(p^2)$.

Using the above matrices, it is easy to check that the relation

$$(x_o\, y_o^{(p+1)/2}\, x_o^2)^3 = 1 \qquad (5.4)$$

holds in (5.1).

Now,
$$x_o\, y_o^{(p+1)/2}\, x_o = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

As,
$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & -\beta \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ \beta & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -\beta & 1 \end{bmatrix}$$

then

$$x_o\, y_o^{(p+1)/2} x_o\, x_1\, x_o\, y_o^{(p+1)/2} x_o = y_1^{(p+1)/2} \qquad (5.5)$$

holds in (5.1). Add the relations (5.3), (5.4) and (5.5) to the presentation (5.1). Let $w = x_o\, y_o^{(p+1)/2} x_o$. (5.6)

By (5.4) and (5.3) we have

$$w^2 = (wx_o)^3 = 1 \tag{5.7}$$

Add the relations (5.6) and (5.7) to (5.1). Our relations are,

$$x_o^p = y_o^p = x_1^p = y_1^p = [x_o,x_1] = [y_o,y_1] = (x_o y_o^{(p+1)/2} x_o)^2 = 1$$

$$(x_o y_o^{(p+1)/2} x_o^2)^3 = w^2 = (wx_o)^3 = 1,\ w = x_o y_o^{(p+1)/2} x_o,$$

$$(x_o^a\, x_1^b\, y_o^c\, y_1^d)^2 = 1,\quad y_1^{(p+1)/2} = x_o y_o^{(p+1)/2} x_o\, x_1\, x_o y_o^{(p+1)/2} x_o.$$

From (5.6) we have

$$y_o^{(p+1)/2} = x_o^{-1} w\, x_o^{-1} = w\, x_o\, w$$

which implies $$y_o = w\, x_o^2\, w\ . \tag{5.8}$$

Also, $$y_1^{(p+1)/2} = w\, x_1 w$$

which implies $$y_1 = w\, x_1^2\, w. \tag{5.9}$$

We eliminate y_o and y_1 using (5.8) and (5.9). Our defining relations are:

$$x_o^p = x_1^p = w^2 = (wx_o)^3 = [x_o,x_1] = 1 \tag{5.10}$$

$$(w\, x_o^2 w)^p = (w\, x_1^2 w)^p = 1 \tag{5.11}$$

$$[w\, x_o^2\, w,\ w\, x_1^2 w] = 1 \tag{5.12}$$

$$(x_o (wx_o^2 w)^{(p+1)/2}\, x_o)^2 = (x_o (wx_o^2 w)^{(p+1)/2} x_o^2)^3 = 1 \tag{5.13}$$

$$w = x_o (wx_o^2 w)^{(p+1)/2} x_o \tag{5.14}$$

$$(w\, x_1^2 w)^{(p+1)/2} = x_o (wx_o^2 w)^{(p+1)/2} x_o x_1 x_o (wx_o^2 w)^{(p+1)/2} x_o \tag{5.15}$$

$$(x_o^a\, x_1^b\, (wx_o^2 w)^c (wx_1^2 w)^d)^2 = 1 \tag{5.16}$$

Clearly the relations in (5.11) are redundant since $w^2 = 1$ and $x_i^p = 1$. Now,

$$w\, x_o^2 w\, w\, x_1^2 w\, w\, x_o^{-2} w\, w\, x_1^{-2} w$$

$$= w\, x_o^2\, x_1^2\, x_o^{-2}\, x_1^{-2}\, w \quad (\text{since } w^2 = 1)$$

$$= 1.$$

Hence (5.12) is redundant.

$$(x_o(wx_o^2\, w)^{(p+1)/2}\, x_o)^2 = (x_o\, w\, x_o\, w\, x_o)^2 = w^2 = 1 \text{ (since } (wx_o)^3=1).$$

$$(x_o(wx_o^2\, w)^{(p+1)/2}\, x_o^2)^3 = (x_o\, w\, x_o\, w\, x_o\, x_o)^3 = (wx_o)^3 = 1\ ,$$

and so (5.13) is redundant.

$$x_o(wx_o^2w)^{(p+1)/2}x_o = x_o w\, x_o w\, x_o = w \quad (\text{since } (wx_o)^3 = 1)$$

showing (5.14) is redundant.

$$x_o(wx_o^2w)^{(p+1)/2}x_o\, x_1\, x_o(wx_o^2w)^{(p+1)/2}\, x_o$$

$$= x_o w\, x_o w\, x_o\, x_1\, x_o w\, x_o w\, x_o = w\, x_1\, w = (wx_1^2w)^{(p+1)/2}$$

and so (5.15) is redundant.

(5.16) becomes,

$$(x_o^a\, x_1^b\, w\, x_o^{2c}\, x_1^{2d}\, w)^2 = 1.$$

Finally, writing x_o as x and x_1 as y proves the theorem.

Definition 5.4

As before, $\forall\ f \in GF(p^2)^*$, we define X_f to be

$$X_f = \{g \in GF(p^2)\ ;\ gf - 1 = x^r\}$$

Definition 5.5

The set of elements $f \in GF(p^2)^* \setminus \{x^r\ ;\ r = 1,2,\ldots,2p-2\}$ will be called the depleted set and denoted by $D(p^2)$. We note that every $f \in D(p^2)$ has the form a+bx, $a,b \neq 0$.

Lemma 5.6

$$X_{fx^r} = x^{-r}X_f.$$

Proof

If $g \in X_f$, then $(gx^{-r})(fx^r) - 1$ is a power of x. That is $gx^{-r} \in X_{fx^r}$.

We shall be mainly concerned with $D(p^2)$ and their X sets. Lemma 5.6 shows we only need to consider elements of the form $1 + q^s x$, for if $f = a + bx$, then $X_f = a^{-1} X_{f'}$ where $f' = 1 + bx/a$.

Theorem 5.7

Let $f = 1 + q^s x$ and k be the order of q^{2s+1} in GF(p). Then, there are elements $h_j \in X_f$, $j = 1,2,\ldots,2k$ with the property that

(i) h_j is obtained from h_{j-1} by adding on a power of x.

(ii) $h_1 = 1$, $h_{2k-1} = xq^{-s-1}$, $h_{2k} = 0$.

(iii) $h_k = 2f^{-1}$.

Proof

Since $f = 1 + q^s x$, then $1 \in X_f$. Let $h_1 = 1$. Define

$$h_{2j} = 1 - q^s x + q^{2s} x^2 - \ldots - q^{(2j-1)s} x^{2j-1} = \frac{1 - q^{2js} x^{2j}}{1 + q^s x}$$

and

$$h_{2j+1} = 1 - q^s x + q^{2s} x^2 - \ldots + q^{2js} x^{2j} = \frac{1 + q^{(2j+1)s} x^{2j+1}}{1 + q^s x}$$

It is clear that $h_i \in X_f$ and that (i) is satisfied.

$h_m = 0$ only when m is even. So, $h_{2n} = 0$ whenever $q^{2ns} x^{2n} = 1$. That is $q^{n(2s+1)} = 1$, and so $n = k$. Hence, $h_{2k} = 0$.

$$h_{2k-1} = \frac{1 + q^{(2k-1)s} x^{2k-1}}{1 + q^s x} = \frac{1 + q^{2ks-s+k-1} x}{1 + q^s x} = \frac{1 + q^{-1-s} x}{1 + q^s x}$$

$$= q^{-1-s} x \frac{(1 + q^s x)}{1 + q^s x} = q^{-1-s} x.$$

Finally, $2f^{-1} \in X_f$ and its action on f is to map it to 1, since $2f^{-1} f - 1 = 1$. Now, $p-1 \mid k(2s+1)$. As $2 \mid p-1$, then k is even as $2s+1$ is odd. $h_k f - 1 = -q^{ks} x^k = -q^{m(2s+1)}$ where $2m = k$. But, $q^{k(2s+1)} = 1$ and so $q^{m(2s+1)} = -1$. Hence, $h_k f - 1 = 1$, and so $h_k = 2f^{-1}$.

Remarks

As in previous chapters, we could have defined X_f to be useful. However, it is not neccessary here. Interestingly enough, the only elements for which X_f is useful are of the form $(1+q^s x)a$ or $(1+q^s x)ax$ where $(2s+1,p-1) = 1$ and $a \in GF(p)$.

We are now ready to prove a result which has always evaded us in other chapters.

Theorem 5.8

$G_{q,p}$ is isomorphic with $PSL(2,p^2)$.

Proof

Let $G = G_{q,p}$ and $H = \langle a, b, d \rangle$. a and b generate an abelian group of order p^2. We can associate the word $a^n b^m$ with the expression A^{n+mx}, $n,m \in GF(p)$ and x satisfying $m_q(x) = 0$. Now, as

$$d\ a\ d^{-1} = a^q \text{ and } d\ b\ d^{-1} = b^q$$

then

$$d\ A^n\ d^{-1} = A^{nq} \text{ and } d\ A^{mx}\ d^{-1} = A^{mqx}$$

and

$$d\ A^{n+mx}\ d^{-1} = d\ A^n\ d^{-1}\ d\ A^{mx}\ d^{-1} = A^{(n+mx)q}. \qquad (5.17)$$

Therefore, any word in H can be written as

$$d^r\ A^{n+mx}, \quad r = 1,2,\ldots,p-1\ ,\ n,m \in GF(p).$$

Hence, $|H| \leq p^2(p-1)$. The rest of the proof follows in four stages.

(i) $PSL(2,p^2)$ is a homomorphic image of G. To see this, consider the map ϕ: G$\longrightarrow$ $PSL(2,p^2)$ given by,

$$a \longmapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ b \longmapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},\ c \longmapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ d \longmapsto \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$$

where x satisfies $x^2 = q$. It is easy to check that these matrices

satisfy the relations of G. Therefore, by the substitution test, ϕ extends to a homomorphism ϕ': G $\longrightarrow$ PSL(2,p^2). By Beetham's results [1], we know $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, $\begin{pmatrix}1 & 0\\ -2 & 1\end{pmatrix}$, $\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}$ and $\begin{pmatrix}1 & 0\\ -2x & 1\end{pmatrix}$ generate PSL(2,p^2). If we can show that these can be expressed in terms of $a\phi$, $b\phi$, $c\phi$ and $d\phi$, it follows that ϕ' is an epimorphism. The first and third of these are already in this form.

$$\begin{pmatrix}1 & 0\\ -2 & 1\end{pmatrix} \equiv \begin{pmatrix}-1 & 0\\ 2 & -1\end{pmatrix} = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^2\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} = c\phi(a\phi)^2c\phi.$$

$$\begin{pmatrix}1 & 0\\ -2x & 1\end{pmatrix} \equiv \begin{pmatrix}-1 & 0\\ 2x & -1\end{pmatrix} = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}^2\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} = c\phi(b\phi)^2c\phi.$$

(ii) If $N \trianglelefteq G$ is such that $G/N \equiv PSL(2,p^2)$, then $H \cap N = 1$.

For, $HN/N = \left\langle \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}, \begin{pmatrix}x & 0\\ 0 & x^{-1}\end{pmatrix} \right\rangle$ is the subgroup of upper triangular matrices in PSL(2,p^2) and has order $p^2(p-1)$. Now, $HN/N \equiv H/(H \cap N)$ and since $|H| = p^2(p-1)$, then $H \cap N = 1$.

(iii) We shall show the words

$$(c\ a^e b^f c\ a^{2g} b^{2h})^2 \in H$$

where $(e+fx)(g+hx) = 1$ in GF(p^2). Consider the cosets of H. $Ha = Hb = Hd = H$. Define new cosets HcA^f, where $f \in GF(p^2)$. Then,

$$H\ c\ A^f\ a = H\ c\ A^{f+1}$$
$$H\ c\ A^f\ b = H\ c\ A^{f+x}.$$

Using (5.17),

$$H\ c\ A^f\ d^{-1} = H\ c\ d^{-1}\ A^{fq} = H\ d\ c\ A^{fq} = H\ c\ A^{fq}.$$

So, $H\ c\ A^f\ d = H\ c\ A^{fq^{-1}}$. Let $r = q^{-1}$. We note that (using lemma 1.32)

$$H\ c\ A^f\ d^n = H\ c\ A^{fr^n}.$$

So, a, b and d just permute these cosets.

$$H\ c\ a\ c = H\ a^{-1}c\ a^{-1} = H\ c\ a^{-1}.$$

$$H\ c\ a^{q^n}c = H\ c\ d^n a\ d^{-n}c = H\ d^{-n}c\ a\ c\ d^n$$

$$= H\ c\ a\ c\ d^n = H\ c\ a^{-1}d^n$$

$$= H\ c\ a^{-r^n}. \qquad (5.18)$$

As $(bdc)^3 = 1$, then

$$c\ b\ c = d^{-1}b^{-1}c\ d^{-1}b^{-1}d = d^{-1}b^{-1}c\ b^{-r} \qquad (5.19)$$

Therefore,

$$H\ c\ b\ c = H\ d^{-1}b^{-1}c\ b^{-r} = H\ c\ b^{-r}.$$

$$H\ c\ b^{q^n}c = H\ c\ d^n b\ d^{-n}c = H\ c\ b\ c\ d^n$$

$$= H\ c\ b^{-r}d^n$$

$$= H\ c\ b^{-r^{n+1}}. \qquad (5.20)$$

(5.18) and (5.20) combine into the single expression

$$H\ c\ A^{x^r}c = H\ c\ A^{-x^{-r}}.$$

This shows we get no new cosets from $H\ c\ A^f$ when f is a power of x. Now, for all $f \in D(p^2)$, define the cosets HcA^fcA^g where $g \in GF(p^2)$.

$$H\ c\ A^f c\ A^g a = H\ c\ A^f c\ A^{g+1}.$$

$$H\ c\ A^f c\ A^g b = H\ c\ A^f c\ A^{g+x}$$

$$H\ c\ A^f c\ A^g d = H\ c\ A^f c\ d\ A^{gr}$$

$$= H\ c\ A^f d^{-1}c\ A^{gr}$$

$$= H\ c\ A^{fq}c\ A^{gr},$$

showing a, b and d permute these cosets.

$$H\ c\ A^f c\ a\ c = H\ c\ A^f a^{-1}c\ a^{-1} = H\ c\ A^{f-1}c\ a^{-1}.$$

$$H\ c\ A^f c\ a^{q^n}c = H\ c\ A^f c\ d^n a\ d^{-n}c$$

$$= H\ c\ A^f d^{-n}c\ a\ c\ d^n$$

$$= H\ c\ A^{fq^n}c\ a\ c\ d^n$$

$$= H\ c\ A^{fq^n-1}c\ a^{-1}d^n$$

$$= H\ c\ A^{(fq^n-1)q^n}c\ a^{-r^n}. \qquad (5.21)$$

Using (5.19) we have,

$$H\ c\ A^f c\ b\ c = H\ c\ A^f d^{-1}b^{-1}c\ b^{-r}$$

$$= H\ c\ A^{fq-x}c\ b^{-r}$$

$$= H\ c\ A^{(fx-1)x}c\ b^{-r}.$$

$$H\ c\ A^f c\ b^{q^n}c = H\ c\ A^f c\ d^n b\ d^{-n}c$$

$$= H\ c\ A^f d^{-n}c\ b\ c\ d^n$$

$$= H\ c\ A^{fq^n}c\ b\ c\ d^n$$

$$= H\ c\ A^{f'}c\ b^{-r}d^n \quad \text{where } f' = (fq^n x-1)x$$

$$= H\ c\ A^{f'q^n}c\ b^{-r^{n+1}}. \qquad (5.22)$$

(5.21) and (5.22) can be combined into the single expression,

$$H\ c\ A^f c\ A^{x^r}c = H\ c\ A^{(fx^r-1)x^r}c\ A^{-x^{-r}}.$$

Now consider elements of X_f. Let $f = 1 + q^s x$. By theorem 5.7, the elements $h_j \in X_f$, $j = 1,2,\ldots,2k$. Let $g = h_i$ for some i. Suppose we can show

$$H\ c\ A^f\ c\ A^g c = H\ c\ A^{f(1-fg)^{-1}} \qquad (5.23)$$

Then $h_{1+i} = h_i + x^r = h$, say.

$$H\ c\ A^f c\ A^h c = H\ c\ A^f c\ A^{g+x^r}c$$

$$= H\ c\ A^f c\ A^g c\ c\ A^{x^r}c$$

$$= H\ c\ A^{f'}c\ A^{x^r}c \quad (f' = f(1-fg)^{-1})$$

$$= H\ c\ A^{(f'x^r-1)x^r}c\ A^{-x^{-r}}.$$

But, $f'x^r - 1 = \dfrac{fx^r}{1-fg} - 1 = \dfrac{f(x^r+g)\ -1}{1-fg} = \dfrac{fh\ -\ 1}{1\ -\ fg}$

which is a power of x since $h, g \in X_f$. Therefore, $(f'x^r-1)x^r$ is also a power of x. Letting $(f'x^r - 1)x^r = f''$, we have:

$$H\ c\ A^{f}c\ A^{h}c = H\ c\ A^{f''}c\ A^{-x^{-r}}$$

$$= H\ c\ A^{-f''^{-1}-x^{-r}}.$$

But, $$-f''^{-1} - x^{-r} = -x^{-r}\left(1 + \frac{fg - 1}{1 - fh}\right)$$

$$= \frac{-x^{-r}}{1 - fh}(fg - fh)$$

$$= \frac{-x^{-r}f(-x^{-r})}{1 - fh}$$

$$= f/(1-fh).$$

Hence,

$$H\ c\ A^{f}c\ A^{h}c = H\ c\ A^{f(1-fh)^{-1}}.$$

It follows that if we can show (5.23) holds for h_1, then it holds for all h_j, $j = 1,2,\ldots,2k$. Now, $h_1 = 1$. So,

$$H\ c\ A^{f}c\ A\ c = H\ c\ A^{f-1}c\ A^{-1} = H\ c\ A^{q^{s}x}\ c\ A^{-1}$$

$$= H\ c\ A^{-q^{-s-1}x-1}.$$

But, $-1 - q^{-s-1}x = -q^{-s-1}x(1+q^{s}x) = f(1-f)^{-1}$, and we are finished. As $2f^{-1} = h_k$, we have,

$$H\ c\ A^{f}c\ A^{2f^{-1}}\ c = H\ c\ A^{-f}.$$

Therefore,

$$c\ A^{f}c\ A^{2f^{-1}}\ c\ A^{f}c\ A^{2f^{-1}} \in H.$$

That is,

$$(c\ A^{f}c\ A^{2f^{-1}})^{2} \in H \tag{5.24}$$

When f is of the form $\alpha + \beta x$ then letting $\alpha = q^{t}$, we have

$$H\ c\ A^{f}c\ A^{g}c = H\ c\ A^{fq^{-t}}\ c\ A^{gq^{t}}\ c\ d^{-t}$$

and so by the previous arguments, (5.24) holds in this case too. When f is a power of x, then

$$H\ c\ A^{x^{r}}\ c\ A^{2x^{-r}}\ c = H\ c\ A^{-x^{-r}+\ 2x^{-r}}\ c$$

$$= H\ c\ A^{x^{-r}}\ c$$

$$= H\ c\ A^{-x^r}$$

and so again we have

$$(c\ A^{x^r}\ c\ A^{2x^{-r}})^2 \in H.$$

Therefore, for all $f \in GF(p^2)^*$,

$$(c\ A^{f}\ c\ A^{2f^{-1}})^2 \in H.$$

Rewriting f as e + fx, then

$$(c\ a^e b^f\ c\ a^{2g} b^{2h})^2 \in H \qquad (5.25)$$

where $(e+fx)(g+hx) = 1$ in $GF(p^2)$.

(iv) Finally, we show that G is $PSL(2,p^2)$. Add on the relations

$$(c\ a^e b^f c\ a^{2g} b^{2h})^2 = 1 \qquad (5.26)$$

to G and denote this group by $\overline{G}$. By theorem 5.3, a, b and c, subject to the relations (5.26) and

$$a^p = b^p = c^2 = (ac)^3 = [a,b] = 1\ ,$$

generate a group isomorphic with $PSL(2,p^2)$. Now, from (5.19),

$$d = b^{-1} c\ b^{-r} c\ b^{-1} c$$

and so $G = \langle a,b,c \rangle$ and so $\overline{G} = \langle a,b,c \rangle$. Hence, $\overline{G}$ is either trivial or $PSL(2,p^2)$. However, $\overline{G}$ is not trivial (by extending part (i) of this proof). Hence $\overline{G} \cong PSL(2,p^2)$.

Therefore, the words in (5.25) are elements of $H \cap N$. But by part (ii), $H \cap N = 1$. Therefore, the relations (5.26) hold in G and so G is $PSL(2,p^2)$.

Theorem 5.9

$PSL(2,p^2)$ is isomorphic with

$$\langle a,\ b,\ c \mid c^2 = (ac)^3 = b^p = a^p = [a,b] = (b^2 c b^r c)^2 = (bcb^r c)^3 = 1,$$

$$c\ b\ c\ b^r c\ a\ c\ b^{-r} c\ b^{-1} c = a^r \rangle$$

where r is a primitive element of GF(p).

Proof

$G_{q,p}$ is $PSL(2,p^2)$. Let $rq \equiv 1 \pmod p$. Defining relations for $PSL(2,p^2)$ on generators a, b, c and d are:

$$c^2 = b^p = a^p = (ac)^3 = [a,b] = 1 \tag{5.27}$$

$$(bdc)^3 = 1 \tag{5.28}$$

$$d^{p-1} = 1 \tag{5.29}$$

$$d\,a\,d^{-1} = a^q,\ d\,b\,d^{-1} = b^q,\ (cd)^2 = 1 \tag{5.30}$$

Now,

$$d^s(ac)^3d^{-s} = 1$$

$$\Rightarrow a^{q^s}\ c\ d^{-s}a\ c\ a\ c\ d^{-s} = 1$$

$$\Rightarrow a^{q^s}\ c\ a^{q^{-s}}\ c\ a^{q^s}\ c = d^{2s}.$$

In particular, with $s = (p-1)/2$, $d^{p-1} = (a^{-1}c)^3 = 1$, since $q^s \equiv -1 \pmod p$. Hence, (5.29) is redundant.

$$b\ d\ c\ b\ d\ c\ b\ d\ c = 1$$

$$\Leftrightarrow b\ c\ d^{-1}b\ d\ c\ b\ c = d$$

$$\Leftrightarrow b\ c\ b^r c\ b\ c = d \tag{5.31}$$

We eliminate d using (5.31). The relations (5.27) together with

$$(b^2cb^rc)^2 = 1 \tag{5.32}$$

$$b\ c\ b^r c\ b\ c\ a\ c\ b^{-1}c\ b^{-r}c\ b^{-1} = a^q \tag{5.33}$$

$$b\ c\ b^r c\ b\ c\ b\ c\ b^{-1}c\ b^{-r}c\ b^{-1} = b^q \tag{5.34}$$

are sufficient to define $PSL(2,p^2)$.

Now, (5.34) holds if and only if,

$$b\ c\ b^r c\ b\ c\ b^r\ c\ b^{-1}c\ b^{-r}c\ b^{-1} = b \text{ since } b^p = 1$$

$$\Leftrightarrow b\ c\ b^r c\ b\ c\ b^r c\ b\ c\ b^r c\ b = b \quad \text{(using (5.32))}$$

$$\Leftrightarrow (b\ c\ b^r c)^3 = 1. \tag{5.35}$$

So we replace (5.34) by (5.35). Finally, (5.33) holds if and only if,

$$b\ c\ b^r c\ b\ c\ a^r c\ b^{-1}c\ b^{-r}c\ b^{-1} = a \quad \text{(since } a^p = 1\text{)}$$

$$\Leftrightarrow a^r = c\ b^{-1}c\ b^{-r}c\ b^{-1}a\ b\ c\ b^r c\ b\ c$$

$$\Leftrightarrow a^r = b^r c\ b\ c\ b^r c\ a\ c\ b^{-r} c\ b^{-1} c\ b^{-r}$$

$$\Leftrightarrow a^r = c\ b\ c\ b^r c\ a\ c\ b^{-r} c\ b^{-1} c \quad \text{(since } [a,b] = 1\text{)}$$

This completes the proof.

Corollary 5.10

$PSL(2,p^2)$ is isomorphic with

$$\langle a, b, c \mid c^2 = a^p = b^p = [a,b] = (ac)^3 = (bcb^{2r}c)^2 = (b^2cb^rc)^2 = 1,$$
$$c\ b\ c\ b^r c\ a\ c\ b^{-r} c\ b^{-1} c = a^r \rangle$$

Proof

In theorem 5.9, put $b = y$, $cbc = x$. Then, $y^p = x^p = (y^2x^r)^2 = 1$. By lemma 1.30, $(yx^r)^3 = 1 \Leftrightarrow (yx^{2r})^2 = 1$. That is, $(bcb^rc)^3 = 1 \Leftrightarrow (bcb^{2r}c)^2 = 1$.

Finally, we obtain efficient presentations for $PSL(2,p^2)$, $p = 5$ and 7, and also for $PSL(2,27)$. These results are heavily dependent on the use of COSET. It is already known that $PSL(2,9)$ is efficient (see [5]).

Theorem 5.11

$PSL(2,25)$ is efficient. An efficient presentation is

$$\langle x, y \mid y^5 = (xy^{-1}xy^2)^4,\ x^3 = (xyx^{-1}y)^2,\ (xy^2x^{-1}y^{-2})^2 = x^3y^5 \rangle$$

Proof

The group $G_{2,5}$ is $PSL(2,25)$, by theorem 5.8. By the remarks following definition 5.2, $PSL(2,25)$ is isomorphic with

$$\langle U, R, S_o, S_1 \mid U^3 = (UR)^2 = (US_o)^2 = S_o^5 = S_1^5 = R^4 = (S_1RU)^3 = 1,$$
$$[S_o,S_1] = 1,\ RS_oR^{-1} = S_o^2,\ RS_1R^{-1} = S_1^2 \rangle$$

Now,
$$S_1R\ U\ S_1R\ U\ S_1R\ U = 1$$
$$\Leftrightarrow S_1U^{-1}R^{-1}S_1R\ U\ S_1U^{-1} = R$$

$$\Leftrightarrow S_1U^{-1}S_1^{-2}U\ S_1U^{-1} = R.$$

Replacing R in the above, the defining relations become:

$$U^3 = S_1^5 = (S_1^2U^{-1}S_1^{-2}U)^2 = (S_1U^{-1}S_1^{-2}US_1U^{-1})^4 = 1 \tag{5.36}$$

$$U^{-1}S_1^{-2}US_1U^{-1}S_1US_1^{-1}U^{-1}S_1^2U = S_1^2 \tag{5.37}$$

$$S_o^5 = (US_o)^2 = [S_o,S_1] = 1$$

$$S_1U^{-1}S_1^{-2}US_1U^{-1}S_oUS_1^{-1}U^{-1}S_1^2US_1^{-1} = S_o^2 \tag{5.38}$$

(5.37) becomes

$$U^{-1}S_1^{-2}US_1U^{-1}S_1US_1^{-1}U^{-1}S_1^2US_1^{-2} = 1$$

$$\Leftrightarrow U^{-1}S_1^{-2}US_1U^{-1}S_1US_1^{-1}S_1^2U^{-1}S_1^{-2}U = 1$$

$$\Leftrightarrow S_1US_1U^{-1}S_1US_1U^{-1} = 1$$

$$\Leftrightarrow (S_1US_1U^{-1})^2 = 1 \tag{5.39}$$

Now, S_1 and U generate PSL(2,25) because from (5.38) we have

$$S_1U^{-1}S_1^{-2}US_1U^{-1}S_o^2US_1^{-1}U^{-1}S_1^2US_1^{-1}S_o = 1$$

which gives

$$S_1U^{-1}S_1^{-2}US_1U^{-1}S_oU^{-1}S_1^{-1}US_1^2U^{-1}S_1^{-1} = 1$$

showing that S_o can be expressed in terms of U and S_1.

Consider the group G_o defined by

$$\langle x, y \mid x^3 = y^5 = (xyx^{-1}y)^2 = (xy^2x^{-1}y^{-2})^2 = (xyx^{-1}yx^{-1}y^{-2})^4 = 1 \rangle \tag{5.40}$$

As x and y satisfy (5.36) and (5.39), then G_o has PSL(2,25) as a homomorphic image. Using COSET, we have found $|G_o : \langle y \rangle| = 1560$ which implies $|G_o| = 7800 = |PSL(2,25)|$. So, G_0 is PSL(2,25).

The last relation in (5.40) can be written as

$(xyx^{-1}yx^{-1}y^{-2})^4 = 1 \Leftrightarrow (y^{-1}xy^{-1}x^{-2}y^{-2})^4 = 1$ (using $(xyx^{-1}y)^2 = 1$)

$\Leftrightarrow (xy^{-1}xy^2)^4 = 1.$

Let G_1 be the group,

$\langle x, y \mid y^5 = (xy^{-1}xy^2)^4 = 1,\ x^3 = (xyx^{-1}y)^2 = (xy^2x^{-1}y^{-2})^2 \rangle$

Using COSET, we know x and $yx^{-1}y$ generate G_1. As x^3 commutes with x and with $xyx^{-1}y$, it commutes with $yx^{-1}y$. So, $x^3 \in Z(G_1)$. Let $A = \langle x^3 \rangle$. $A \leq G_1' \cap Z(G_1)$ since G_1 is perfect. $G_1/A \equiv G_o \equiv$ PSL(2,25). Therefore, G_1 is a stem extension of PSL(2,25). COSET shows that $|G_1 : \langle y \rangle| = 1560$, and as $y^5 = 1$, we deduce that $|G_1| = 7800$ and so G_1 is PSL(2,25).

Let G_2 be the group

$\langle x, y \mid y^5 = (xy^{-1}xy^2)^4,\ x^3 = (xyx^{-1}y)^2,\ (xy^2x^{-1}y^{-2})^2 = x^3y^5 \rangle$

and $B = \langle y^5 \rangle$.

y and $xy^{-1}x$ generate G_2 (this being found using COSET). So, as y^5 commutes with y and $xy^{-1}x$, then $y^5 \in Z(G_2)$. $G_2$is perfect and so $B \leq Z(G_2) \cap G_2'$. G_2 is a stem extension of PSL(2,25) since $G_2/B \equiv G_1$, and so is either PSL(2,25) or SL(2,25), by theorem 1.19.

As $y^5 \in Z(G_2)$, then either $y^5 = 1$ or $y^{10} = 1$. In either case, the relation $y^{10} = 1$ holds in G_2. Also, $[y^5,x] = 1$ holds in G_2. Using this information, COSET found

$$|G_2 : \langle y \rangle| = |G_2 : \langle y^2 \rangle| = 1560.$$

But as $\langle y^2 \rangle \leq \langle y \rangle$ we must have $y^5 = 1$. Hence G_2 is isomorphic with PSL(2,25).

Theorem 5.12

PSL(2,49) is efficient. An efficient presentation for it is,

$\langle U, T \mid U^3 = (TU^{-1})^7,\ T^5 = (UT^2UT)^3, (T^2UT^2UTU^{-1})^2 = (T^2U)^5 \rangle$

Proof

The polynomial x^2-x-1 is irreducible over GF(7). The root x, satisfies $x^{16} = 1$. The polynomial is not primitive. However, using the presentation in corollary 4.7, we have

$\langle U, R, S_o, S_1 \mid U^3 = S_o^7 = S_1^7 = R^8 = (UR)^2 = (US_o)^2 = [S_o,S_1] = 1,$

$$(S_1RU)^3 = 1,\ RS_oR^{-1} = S_oS_1,\ RS_1R^{-1} = S_1RS_oR^{-1}\ \rangle$$

is PSL(2,49). This is because the index of $\langle R, S_o, S_1\rangle$ is found to be 150 using COSET. Also, using COSET, $|\langle R,S_o,S_1\rangle| =$ 392 and so this group has order at most 58,800. PSL(2,49) is a homomorphic image as is seen by taking the corresponding matrices to be

$$U \longleftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},\ S_o \longleftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ S_1 \longleftrightarrow \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},\ R \longleftrightarrow \begin{pmatrix} x & x^{-1} \\ 0 & x^{-1} \end{pmatrix}$$

where x satisfies $x^2 = 1+x$.

$$S_1RUS_1RUS_1RU = 1 \Leftrightarrow S_1U^{-1}R^{-1}S_1RUS_1U^{-1} = R$$

$$\Leftrightarrow S_1U^{-1}S_1S_o^{-1}US_1U^{-1} = R \text{ using } RS_1 = S_1RS_o.$$

From $RS_1 = S_1RS_o$ we obtain

$$S_1U^{-1}S_1S_o^{-1}US_1U^{-1}S_1 = S_1^2U^{-1}S_1S_o^{-1}US_1U^{-1}S_o.$$

Using $(US_o)^2 = [S_o,S_1] = 1$, this becomes

$$US_1US_1U^{-1}S_1 = S_1US_1US_1U^{-1}S_o.$$

That is,

$$S_o = US_1^{-1}U^{-1}S_1^{-1}U^{-1}S_1^{-1}US_1US_1U^{-1}S_1.$$

Therefore,

$$R = S_1U^{-1}S_1S_1^{-1}US_1^{-1}U^{-1}S_1^{-1}U^{-1}S_1US_1US_1U^{-1}US_1U^{-1}$$

$$= U^{-1}S_1^{-1}U^{-1}S_1US_1US_1^2U^{-1}.$$

Replacing R and S_o, the defining relations for PSL(2,49) become:

$$U^3 = S^7 = (S^{-1}U^{-1}SUSUS^2U)^8 = (US^{-1}U^{-1}S^{-1}U^{-1}S^{-1}USUSU^{-1}S)^7 = 1$$

$$[S,\ US^{-1}U^{-1}S^{-1}U^{-1}S^{-1}USUSU^{-1}S] = (S^{-1}U^{-1}SUSUS^2U^{-1})^2 = 1,$$

$$(U^{-1}S^{-1}U^{-1}S^{-1}U^{-1}S^{-1}USUSU^{-1}S)^2 = 1, \text{ and}$$

$$USUSU^{-1}SUS^{-2}U^{-1}S^{-1}U^{-1}S^{-1}USUS^{-1} = 1$$

where we have written S_1 as S.

Let SU = T. The relations become:

$$(TU^{-1})^7 = U^3 = 1 \tag{5.42}$$

$$[TU^{-1},\ U^{-1}T^{-3}UT^2UTU^{-1}] = 1 \tag{5.43}$$

$$(UT^{-1}U^{-1}T^3U^{-1}T)^8 = 1 \tag{5.44}$$

$$(T^{-3}UT^2UTU)^7 = 1 \tag{5.45}$$

$$(T^{-1}U^{-1}T^3U^{-1}TU^{-1})^2 = 1 \tag{5.46}$$

$$(T^{-3}UT^2UTU^{-1})^2 = 1 \tag{5.47}$$

$$UT^2UTUT^{-1}UT^{-3}UTUT^{-1} = 1 \tag{5.48}$$

Now T corresponds to $\begin{pmatrix} x & -1-x \\ 1 & -1 \end{pmatrix}$ and it is easily checked that

$$T^5 = 1 \tag{5.49}$$

We add (5.49) to our list of relations.

(5.43) becomes:

$$[TU^{-1},\ U^{-1}T^2UT^2UTU^{-1}] = 1 \Leftrightarrow TUT^2UT^2UTU^{-1} = U^{-1}T^2UT^2UTU^{-1}TU^{-1}$$

$$\Leftrightarrow \quad TUT^2UT^2 = U^{-1}T^2UT^2UTU$$

$$\Leftrightarrow \quad [UTU,\ T^2UT^2] = 1 \tag{5.50}$$

(5.45) becomes:

$$(T^2UT^2UTU)^7 = (T^2UT^2)^7(UTU)^7 \quad \text{(by (5.50))}$$

But, $(UTU)^7 = U(TU^{-1})^6TU = UUT^{-1}TU = 1$. Hence,

$(T^2UT^2UTU)^7 = (T^2UT^2)^7 = T^2(UT^{-1})^6UT^2 = T^3U^{-1}UT^2 = 1$, and so

(5.45) is redundant.

(5.48) becomes:

$$(UT^2UTUT^{-1})^2 = 1$$

which is (5.46). Hence, (5.48) is redundant.

(5.44) becomes:

$$(UT^{-1}U^{-1}T^{-2}U^{-1}T)^8 = 1 \Leftrightarrow (UUT^{-1}UT^2UTU)^8 = 1 \text{ (using (5.46)}$$

$$\Leftrightarrow (T^2U^{-1})^8 = 1 \tag{5.51}$$

(5.50) becomes:

$UTUT^2UT^2 = T^2UT^2UTU \Leftrightarrow UTUT^2UT^2 = T^2UT^2UTU^{-1}U^{-1}$

$\Leftrightarrow UTUT^2UT^2 = UT^{-1}U^{-1}T^{-2}U^{-1}T^{-2}U^{-1}$ (using (5.47)).

That is, $$(T^2U)^5 = 1 \tag{5.52}$$

So PSL(2,49) can be presented as,

$$\langle U, T \mid U^3 = T^5 = (TU^{-1})^7 = (T^2U)^5 = (UT^2UTUT^{-1})^2 = (T^2U^{-1})^8 = 1,$$
$$(T^2UT^2UTU^{-1})^2 = 1 \rangle \tag{5.53}$$

Using COSET we can show the relation $(T^2U^{-1})^8 = 1$ is redundant.

Again, using the correspondence

$$U \longleftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \quad T \longleftrightarrow \begin{pmatrix} x & -1-x \\ 1 & -1 \end{pmatrix}$$

the relation

$$(UT^2UT)^3 = 1 \tag{5.54}$$

holds in (5.53). On replacing the relation $(UT^2UTUT^{-1})^2 = 1$ by (5.54) we still have a presentation for PSL(2,49) as verified by COSET. Let

$G_o = \langle U,T \mid U^3 = T^5 = (TU^{-1})^7 = (UT^2UT)^3 = 1, (T^2U)^5 = (T^2UT^2UTU^{-1})^2 \rangle$

G_o has PSL(2,49) as a homomorphic image. Also, G_o is perfect. Using COSET we have $G_o = \langle T^2U, TU^{-1} \rangle$. Hence $(T^2U)^5 \in Z(G_o)$ since it commutes with T^2U and TU^{-1}. Let $A = \langle (T^2U)^5 \rangle$.

$A \leq Z(G_o) \cap G_o'$. Also, $G_o/A \cong$ PSL(2,49). G_o is therefore a stem extension of PSL(2,49) and so is either PSL(2,49) or SL(2,49) by theorem 1.19.

Let G_1 be the group

$\langle U,T \mid U^3 = (TU^{-1})^7 = 1, T^5 = (UT^2UT)^3, (T^2U)^5 = (T^2UT^2UTU^{-1})^2 \rangle$

and $B = \langle T^5 \rangle \leq G_1$. Again, by using COSET, we have $G_1 = \langle T, UT^2U \rangle$. Since $T^5 = (UT^2UT)^3$, then T^5 commutes with UT^2U and so $T^5 \in Z(G_1)$. G_1 is perfect and so $B \leq G_1' \cap Z(G_1)$. Also, $G_1/B \cong G_o$. G_1 is a stem extension of G_o and is isomorphic with PSL(2,49) or SL(2,49) by theorem 1.19. We are unable to determine the index of TU^{-1} in

G_1. However, as the centre of G_1 is C_2 or trivial, then we know the relations $T^{10} = [U,T^5] = 1$ hold in G_1. Moreover, using this information, we can show that $G_1 = \langle T^2U, TU^{-1} \rangle$ and so $G_1 = \langle T^2U, T^2UT^2UTU^{-1} \rangle$. Hence, $(T^2U)^5$ is central in G_1. The relations $(T^2U)^{10} = [U,(T^2U)^5] = [T,(T^2U)^5] = 1$ hold in G_1. Using this information we have found that $|G_1 : \langle TU^{-1} \rangle| = 8400$ and so $|G_1| \leq 58,800 = |PSL(2,49)|$. G_1 is therefore PSL(2,49).

Finally, let

$$G_2 = \langle U,T \mid U^3 = (TU^{-1})^7,\ T^5 = (UT^2UT)^3,\ (T^2UT^2UTU^{-1})^2 = (T^2U)^5 \rangle$$

and $C = \langle U^3 \rangle$. G_2 is perfect. As U and TU^{-1} generate G_2 then U^3 is central. Hence, $C \leq G_2' \cap Z(G_2)$. $G_2/C \equiv G_1 \equiv PSL(2,49)$.

As with the above arguments, the relations

$$U^6 = (TU^{-1})^{14} = [T,U^3] = 1$$

hold in G_2. With this, and the above information, we have obtained from COSET, that

$$|G_2 : \langle TU^{-1} \rangle| = |G_2 : \langle (TU^{-1})^2 \rangle| = 8400.$$

Therefore, $|G_2| \leq 58,800$ and so G_2 is PSL(2,49).

Although the next result is a little out of place, it is included here as it almost completes the proof that finite simple groups of order $< 10^5$ are efficient. We shall say more about this later.

Theorem 5.13

PSL(2,27) is efficient. An efficient presentation is

$$\langle R, T \mid R^2 = T^{13} = (RT^4)^3,\ (RT^{-1}RT^5)^3 = (RT^{-1}RT^2RT^5)^2R^2 \rangle$$

Proof

We first of all remark that this presentation is not derived from Todd's. Sinkov [16] gives the following presentation for

PSL(2,27).

$\langle P, Q \mid P^{13} = (QP^3)^2 = (QP^2)^3 = (Q^2P^5QP^9)^2 = (Q^2P^9QP^5)^2 = 1 \rangle$

Since $P^{13} = 1$, then P^3 and Q generate. Writing P^3 as T the relations become,

$T^{13} = (QT)^2 = (QT^5)^3 = (Q^2T^6QT^3)^2 = (Q^2T^3QT^6)^2 = 1$, and letting $R^{-1} = QT$ we obtain

$$\langle R,T \mid T^{13} = R^2 = (RT^4)^3 = (RT^{-1}RT^5RT^2)^2 = (RT^{-1}RT^2RT^5)^2 = 1 \rangle \tag{5.55}$$

as a presentation for PSL(2,27). We have been able to show (using COSET) that $(RT^{-1}RT^5)^3 = 1$ holds in (5.55). Moreover, if we add this relation to (5.55) we can remove the relation $(RT^{-1}RT^5RT^2)^2 = 1$. Hence, PSL(2,27) has the following presentation:

$\langle R, T \mid T^{13} = R^2 = (RT^4)^3 = (RT^{-1}RT^5)^3 = (RT^{-1}RT^2RT^5)^2 = 1 \rangle$

Let G_o be the group

$\langle R, T \mid T^{13} = R^2 = (RT^4)^3 = 1, (RT^{-1}RT^5)^3 = (RT^{-1}RT^2RT^5)^2 \rangle$

and $A = \langle (RT^{-1}RT^5)^3 \rangle$. G_o is generated by $RT^{-1}RT^5$ and $RT^{-1}RT^2RT^5$. This was found using COSET. Therefore, $(RT^{-1}RT^5)^3 \in Z(G_o)$. G_o is perfect and since $G_o/A \cong PSL(2,27)$ then G_o is a stem extension of PSL(2,27). G_o then, is either PSL(2,27) or SL(2,27) and so the centre of G_o is trivial or C_2. In either case, the relations $[(RT^{-1}RT^5)^3, T] = (RT^{-1}RT^2RT^5)^4 = 1$ hold in G_o. Using this information, when we applied COSET, we found $|G_o : \langle T \rangle| = 756$. Therefore, $|G_o| \leq 9828 = |PSL(2,27)|$. Hence, G_o is isomorphic with PSL(2,27). Let G_1 be the group

$\langle R, T \mid R^2 = T^{13} = (RT^4)^3, (RT^{-1}RT^5)^3 = (RT^{-1}RT^2RT^5)^2R^2 \rangle$.

Since G_1 is generated by R and T, then T^{13} and R^2 are central. Let $B = \langle T^{13} \rangle$. $B \leq Z(G_1) \cap G_1'$ since G_1 is perfect. Also, $G_1/B \cong G_o \cong PSL(2,27)$. Therefore, G_1 is a stem extension of PSL(2,27) and so by theorem 1.19, is PSL(2,27) or SL(2,27).

Since $Z(G_1)$ is either C_2 or trivial, then the relations

$$[R^2,T] = [T^{13}, R] = R^4 = 1$$

hold in G_1. Using this and the above information, we have found using COSET that

$$|G_1 : \langle T \rangle| = |G_1 : \langle T^2 \rangle| = 756.$$

As $T^{26} = 1$, then we must have $T^{13} = 1$ since $\langle T \rangle = \langle T^2 \rangle$. Therefore, $|G_1| = 9828 = |PSL(2,27)|$, and so $G_1 \equiv PSL(2,27)$.

Remark

1. Since these results, Campbell has also found efficient presentations for PSL(2,25) and PSL(2,27), [13].

2. Campbell and Robertson [5] have found efficient presentations for all the finite simple groups of order $<10^5$ except for M_{11}, PSU(3,3) and the PSL groups. They have also found efficient presentations for SL(2,8) and SL(2,16). With the above results, this means that all finite simple groups of order $<10^5$, except M_{11}, PSU(3,3) and SL(2,32) have been proved efficient.

References

1. M.J. Beetham, " A set of generators and relations for the groups PSL(2,q), q odd", J. London Math. Soc., (2) 3 (1971), 554-557.
2. H. Behr and J. Mennicke, "A presentation of the groups PSL(2,q)", Canad. J. Math., 20 (1968), 1432-1438.
3. C.M. Campbell and E.F. Robertson, "A deficiency zero presentation for SL(2,p)", Bull. London Math. Soc., 12 (1980), 17-20.
4. C.M. Campbell and E.F. Robertson, "Two generator, two relation presentations for special linear groups", The Geometric Vein. (Springer-Verlag, New York, Berlin, 1982, 561-568).
5. C.M. Campbell and E.F. Robertson, "The efficiency of simple groups of order $< 10^5$", Comm. Alg., 10 (1982), 217-225.
6. P.M. Cohn, Algebra. (Wiley, London, 1974).

6a. P.M. Cohn, Algebra, vol 2. (Wiley, London, 1977).

7. H.S.M. Coxeter and W.O.J. Moser, Generators and relations for discrete groups, 4^{th} edition. (Springer-Verlag, Berlin 1980).
8. L.E. Dickson, Linear groups with an exposition of the Galois field theory. (Dover, New York, 1958).
9. B. Huppert, Endliche gruppen 1. (Springer, Berlin, 1967).
10. D.L. Johnson, Topics in the theory of group presentations. (C.U.P., L.M.S. Lecture Note Series 42, 1980).
11. J. Mennicke, "On Ihara's modular group", Inventiones Math., 4 (1967), 202-228.
12. I.D. Macdonald, The theory of groups. (O.U.P., 1968).

13. E.F. Robertson, "Efficiency of finite simple groups and their covering groups", Proceedings of 'Finite Groups-Coming of Age' (to appear).

14. I. Schur, "Untersuchungen uber die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen", J. Math., 132 (1907), 85-137.

15. S. Sidki, "HK ∩ KH in groups", Trabalho de Matematica, Universidade de Brasilia, Number 96 (1975).

16. A. Sinkov, "A note on a paper by J.A. Todd", Bull. Amer. Math. Soc., 45 (1939), 762-765.

17. J.G. Sunday, "Presentations of the groups SL(2,m) and PSL(2,m)", Canad. J. Math., 24 (1972), 1129-1131.

18. J.A. Todd, "A note on the linear fractional group", J. London Math. Soc., 7 (1932), 195-200.

19. J.A. Todd, "A second note on the linear fractional group", J. London Math. Soc., 2 (1936), 103-107.

20. H. Zassenhaus, "A presentation of the groups PSL(2,p) with three defining relations", Canad. J. Math., 21 (1969), 310-311.

21. N. Zierler, "On x^n+x+1 over GF(2)", Information and Control, 16 (1970), 502-505.